Fortinet Controller

Installation Guide

Support

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service

Fortinet Product License Agreement / EULA and Warranty Terms

To ensure a secured WiFi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware

Trademarks and Copyright Statement

Product License Agreement

The parties to this agreement are you, the end customer, and either (i) where you have purchased your Product within the Americas, Fortinet, Inc., or (ii) where you have purchased your Product outside of the Americas, Fortinet Singapore Private Limited (each referred to herein as "Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS “AGREEMENT” OR “EULA”). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET’S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT IMMEDIATELY NOTIFY THE FORTINET LEGAL TEAM IN WRITING AT *LEGAL@FORTINET.COM* OF REQUESTED CHANGES TO THIS AGREEMENT.

1. License Grant.

This is a license, not a sales agreement, between you and Fortinet. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet's Products which is discussed in detail in section 15 below, and the term "Software" includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option. Fortinet grants to you a non-transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-exclusive, revocable (in the event of your failure to comply with these terms or in the event Fortinet is not properly paid for the applicable Product) license to use the Software solely for your internal business purposes (provided, if a substantial portion of your business is to provide managed service provider services to your end-customers, you may use the Software embedded in FortiGate and supporting hardware appliances to provide those services, subject to the other restrictions in this Agreement), in accordance with the terms set forth in this Agreement and subject to any further restrictions in Fortinet documentation, and solely on the Fortinet appliance, or, in the case of blades, CPUs or databases, on the single blade, CPU or database on which Fortinet installed the Software or, for stand-alone Software, solely on a single computer running a validly licensed copy of the operating system for which the Software was designed, or, in the case of blades, CPUs or databases, on a single blade, CPU or database. For clarity, notwithstanding anything to the contrary, all licenses of Software to be installed on blades, CPUs or databases are licensed on a per single blade, solely for one blade and not for multiple blades that may be installed in a chassis, per single CPU or per single database basis, as applicable. The Software is "in use" on any Fortinet appliances when it is loaded into temporary memory (i.e. RAM). You agree that, except for the limited, specific license rights granted in this section 1, you receive no license rights to the Software.

2. Limitation on Use.

You may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner; (c) except as provided in section 5, transfer assign or sublicense right to any other person or entity, or (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers.

3. Proprietary Rights.

All rights, title, interest, and all copyrights to the Software and any copy made thereof by you and to any Product remain with Fortinet. You acknowledge that no title to the intellectual property in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific license as expressly set forth in section 1 ("License Grant") above. You agree to keep confidential all Fortinet

confidential information and only to use such information for the purposes for which Fortinet disclosed it.

4. Term and Termination.

Except for evaluation and beta licenses or other licenses where the term of the license is limited per the evaluation/beta or other agreement or in the ordering documents, the term of the license is for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet. The provisions of this Agreement, other than the license granted in section 1 ("License Grant"), shall survive termination.

5. Transfer.

If you are a Fortinet contracted and authorized reseller or distributor of Products, you may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one end user on a permanent basis, provided that: (i) you ensure that your customer and the end user receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, you hereby agree to enforce the terms in this Agreement against such end user, (ii) you at all times comply with all applicable United States export control laws and regulations, and (iii) you agree to refund any fees paid to you by an end user who purchased Product(s) from you but does not agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Further, if you are a non-authorized reseller of Products, you are not authorized to sell Product(s) or Software, but, regardless, by selling Product(s) or Software, you hereby agree you are bound by the restrictions and obligations herein and are bound to: (i) ensure that your customer and the end user receive a copy of this Agreement and are bound in full by all restrictions and obligations herein (ii) enforce the restrictions and obligations in this Agreement against such customer and/or end user, (iii) comply with all applicable United States export control laws and regulations and all other applicable laws, and (iv) refund any fees paid to you by a customer and/or end user who purchased Product(s) from you but does not agree to the restrictions and obligations contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way.

6. Limited Warranty.

Fortinet provides this limited warranty for its product only to the single end-user person or entity that originally purchased the Product from Fortinet or its authorized reseller or distributor and paid for such Product. The warranty is only valid for Products which are properly registered on Fortinet’s Support Website, *https://support.fortinet.com*, or such other website as provided by Fortinet, or for which the warranty otherwise

starts according to Fortinet's policies. The warranty periods discussed below will start according to Fortinet's policies posted at *http://www.fortinet.com/aboutus/legal.html* or such other website as provided by Fortinet. It is the Fortinet distributor's and reseller's responsibility to make clear to the end user the date the product was originally shipped from Fortinet, and it is the end user's responsibility to understand the original ship date from the party from which the end user purchased the product. All warranty claims must be submitted in writing to Fortinet before the expiration of the warranty term or such claims are waived in full. Fortinet provides no warranty for any beta, donation or evaluation Products, for any spare parts not purchased directly from Fortinet by the end-user, for any accessories, or for any stand-alone software. Fortinet warrants that the hardware portion of the Products, including spare parts unless noted otherwise ("Hardware") will be free from material defects in workmanship as compared to the functional specifications for the period set forth as follows and applicable to the Product type ("Hardware Warranty Period"): a three hundred sixty-five (365) day limited warranty for the Hardware excluding spare parts, power supplies, and accessories (provided, solely with respect to FortiAP and Meru AP indoor Wi-Fi access point Hardware appliance products and FortiSwitch Hardware appliance products other than the FortiSwitch-5000 series (for both excluding spare parts, power supplies, and accessories), the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date), and, for spare parts, power supplies, and accessories, solely a ninety (90) days limited warranty. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new or of an identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Hardware Warranty Period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by Fortinet upon return to Fortinet of the defective Hardware. All Hardware (or part thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. Fortinet warrants that the software as initially shipped with the Hardware Products will substantially conform to Fortinet's then current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days ("Software Warranty Period"), if the Software is properly installed on approved Hardware and operated as contemplated in its documentation. Fortinet's sole obligation shall be to repair or offer replacement Software for the non-conforming Software with software that substantially conforms to Fortinet's functional specifications. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Except as otherwise agreed by

Fortinet in writing, the warranty replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by Fortinet for the Software. The Software Warranty Period shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material non-conformance is incapable of correction or that it is not practical to repair or replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by Fortinet; provided that the non-conforming Software (and all copies thereof) is first returned to Fortinet. The license granted respecting any Software for which a refund is given automatically terminates immediately upon refund. For purpose of the above hardware and software warranties, the term “functional specifications” means solely those specifications authorized and published by Fortinet that expressly state in such specifications that they are the functional specifications referred to in this section 6 of this Agreement, and, in the event no such specifications are provided to you with the Software or Hardware, there shall be no warranty on such Software.

7. Disclaimer of Other Warranties and Restrictions.

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE HARDWARE WARRANTY PERIOD DISCUSSED ABOVE DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTITOKEN WHICH HAS A 365 DAY WARRANTY FROM THE DATE OF SHIPMENT FROM FORTINET’S FACILITIES, AND THE SOFTWARE WARRANTY DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTIGATE-ONE AND VDOM SOFTWARE. YOU HEREBY ACKNOWLEDGE AND AGREE THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE. The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee. In the case of beta, testing, evaluation, donation or free Software or Product, the end user acknowledges and agrees that such Software or Product may contain bugs or

errors and could cause system failures, data loss and other issues, and the end user agrees that such Software or Product is provided “as-is” without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever. An end user’s use of evaluation or beta Software or Product is limited to thirty (30) days from original shipment unless otherwise agreed in writing by Fortinet.

8. Governing Law.

Any disputes arising out of this Agreement or Fortinet’s limited warranty shall be governed by the laws of the state of California, without regard to the conflict of laws principles. In the event of any disputes arising out of this Agreement or Fortinet’s limited warranty, the parties submit to the jurisdiction of the federal and state courts located in Santa Clara County, California, as applicable.

9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE-INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THE LIMITED WARRANTY IN SECTION 6 ABOVE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE.

10. Import / Export Requirements; FCPA Compliance.

You are advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws; diversion contrary to United States law and regulation is prohibited. You agree to comply with all applicable international and national laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see *www.bis.doc.gov*. Fortinet assumes no responsibility or liability for your failure to obtain any

necessary import and export approvals, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation. You represent that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against you or otherwise suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by regulation or specific written license. Additionally, you agree not to directly or indirectly export, import or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Furthermore, you represent that you understand, and you hereby agree to comply with, all requirements of the U.S. Foreign Corrupt Practices Act and all other applicable laws. For beta, testing, evaluation, donation or free Products and/or related services, you hereby agree, represent and warrant to Fortinet that (a) receipt of the Products and/or services comply with all policies and you have obtained all necessary approvals for such Products and/or services, (b) the Products and/or services are not provided in exchange for Fortinet maintaining current business or for new business opportunities, and (c) the Products and/or services are not being received for the benefit of, and are not being transferred to, any government entity, representative or affiliate.

11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

12. Tax Liability.

You agree to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

13. General Provisions.

Except as specifically permitted and required in section 5 (“Transfer”) above, you agree not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement and other Fortinet agreements may be amended or supplemented only by a writing that refers explicitly to the agreement signed on behalf of both parties, or, for this Agreement, as otherwise expressly provided in the lead-in above Section 1 above, provided, notwithstanding anything to the contrary and except for this Agreement which may be amended or updated as expressly provided in the lead-in above Section 1 above, for any amendment or other agree-

ment to be binding on Fortinet, such amendment or other agreement must be signed by Fortinet's General Counsel. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, that part will be enforced to the maximum extent permitted and the remainder shall continue in full force and effect. You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions.

14. Privacy.

For information regarding Fortinet's collection, use and transfer of your personal information please read the Fortinet privacy policy on the Fortinet web site (*http://www.fortinet.com/aboutus/privacy.html*).

15. Open Source Software.

Fortinet's products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public License, Version 2, of June 1991 ("GPL") or GNU Lesser General Public License, Version 2.1, of February 1999 ("LGPL") or other open source software licenses which, among other rights, permit the user touse, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on this CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify a Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send your written request, along with a check in the amount of US $25.00, to General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA. In order to receive the modified software modules, you must also include the following information: (a) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules "AS-IS" without warranty of any kind, either expressed or implied. In no event will the copyright holder for the open source software be liable to you for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may obtained by contacting Fortinet's Legal Department at *legal@fortinet.com*.

GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the

Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if

the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under

this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for your own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of

definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this

License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is

given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

15. The warranty disclaimer contained in Sections 11 and 12 of the preceding GPL License is incorporated herein.

Table of Contents

1 About this Guide

This guide describes the features of the controller family as well as the hardware installation procedure for all controllers. The term “controller” is used interchangeably throughout this document to apply to all controllers when there are no differences between the models.

Audience

This guide is intended for system or network administrators responsible for installing the controller. A detailed understanding of networking is not required, however familiarity with the following concepts are helpful in configuring your controller:

- Network administration, including:
  - Internet Protocol (IP) addressing and routing
  - Dynamic Host Configuration Protocol (DHCP)
  - Configuring Layer 2 switches (if required by your switch)
- IEEE 802.11 (Wi-Fi) concepts, including:
  - ESSIDs
  - WEP
- Network Security (optional)
  - 802.1X
  - RADIUS
  - WPA
  - X.509 certificates
- *“Cautions and Warnings”* ***on page 87*** describes cautions and warnings that should be followed prior to using the controller.

Other Sources of Information

Additional information is available in the following documents, Web site, and external references.

Documentation

- *System Director Release Notes*
- *Access Point Installation Guide*
- *System Director Command Reference*
- *System Director Configuration Guide*

External References

- Stevens, W. R. 1994. TCP/IP Illustrated, Volume 1, The Protocols. Addison-Wesley, Reading, Mass.
- Gast, M.S. 2002. 802.11 Wireless Networks, The Definitive Guide. O'Reilly and Associates, Sebastopol, Calif.

Typographic Conventions

This document uses the following typographic conventions to help you locate and identify information:

	Provides extra information, tips, and hints regarding the topic
	Identifies important information about actions that could result in damage to or loss of data, or could cause the application to behave in unexpected ways.
	Identifies critical information about actions that could result in equipment failure or bodily harm.

Contacting Us

Fortinet Web Site

You can visit Fortinet. on the Internet at this URL:

www.fortinet.com

Customer Services and Support

For assistance, contact Customer Services and Support 24 hours a day at +1-888-637-8952 or +1-408-215-5305. Email can be sent to csm@fortinet.com .

Customer Services and Support provide end users and channel partners with the following:

- Telephone technical support
- Software update support
- Spare parts and repair service

RMA Procedures

Contact Customer Services and Support for a Return Material Authorization (RMA) for any Fortinet equipment.

Please have the following available when making a call:

- Company and contact information
- Equipment model and serial numbers
- Software release and revision numbers (for example, 3.0.0-35)
- A description of the symptoms the problem is manifesting
- Network configuration

2 Controller Introduction

Controllers provide the central management and intelligence of an enterprise's wireless LAN networking environment; Controllers are designed to meet performance requirements for smaller networks, while other controllers are designed for larger networks. See the chart below for details.

Controller	Design Objective
MC1500	MC1500 is designed to support small to medium networks with up to 30 Access Points, 500 wireless clients, and a throughput level of up to 800 Mbps supported by two Ethernet connections.
MC1550	MC1550 is a small form-factor controller designed to support small to medium networks with up to 50 Access Points, 1000 wireless clients, and a throughput level of up to 800 Mbps supported by two Ethernet connections.
MC3200	MC3200 controllers are designed for medium enterprise deployments. They support up to 200 Access Points, 2000 wireless clients, and have a throughput level of up to 2 Gbps supported by four Ethernet connections.
MC4200	MC4200 is intended to meet the needs of large enterprises. They support up to 500 Access Points, 5000 wireless clients, and have a throughput level of up to 4 Gbps using a built-in acceleration module and four Ethernet connections. The MC4200 also supports an optional 10G module (purchased separately), which is described in <Xref>Installing the 10G Module (MC4200 Only).
MC5000	MC5000 is a chassis-based Wireless LAN controller targeted to meet the needs of large scale enterprises with high availability. A MC5000 chassis has five slots for controller blades. When used with the optional acceleration module, each controller blade can support up to 300 Access Points, 3000 wireless clients, and have a throughput level of up to 4 Gbps.

Controller	Design Objective
MC6000	MC6000 is a chassis-based Wireless LAN controller targeted to meet the needs of large scale enterprises with high availability. A MC6000 chassis has ten slots for controller blades. Each controller blade can support up to 500 Access Points, 5000 clients, and have a throughput level of up to 10Gbps.
Virtual	Virtual controllers are controller images that can be installed on an existing hardware platform provided that the platform implements a supported virtual hosting software solution. They can be purchased in varying sizes to allow them to be tailored to the needs of your deployment.

All controllers run System Director, that centrally manages and monitors access points (APs). System Director software provides a centralized management system accessed from either the Web UI or a Command Line Interface (CLI) for monitoring, configuration, and troubleshooting the system. In addition, a set of extensible services is provided for security, RF planning, over-the-air QoS for converged data, voice and video networks, zero-loss handoff mobility, and location-based applications. Controllers provide the central management and intelligence of an enterprise's wireless LAN networking environment. Controllers scale to meet performance requirements from small to large enterprises, including support for connecting remote locations with a small number of Access Point that may or may not include a local controller.

3 MC1500 Controller

The MC1500 is designed for small to medium-scale site deployments, such as small offices or remote branch sites. It supports customers requiring Layer 1-4 security, Fast Ethernet, and affordable performance. The MC1500 can support up to 30 APs.

The MC1500 measures 16.7x1.1x10.6 inches. The front and back of the MC1500 are shown below.

Figure 1: *MC1500 Front Panel*

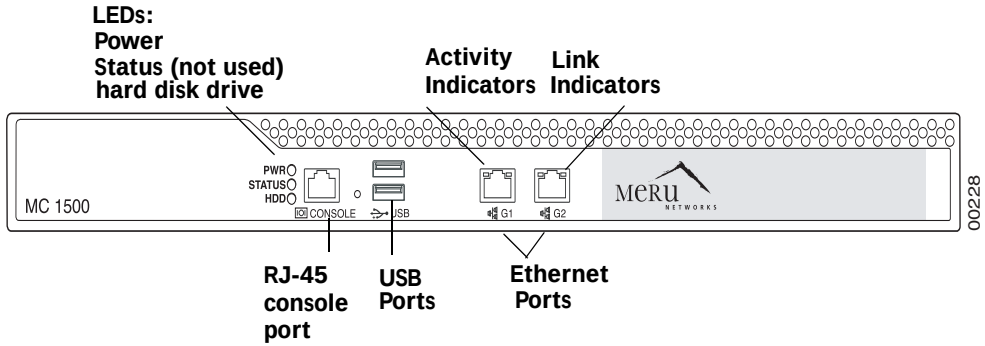


Figure 2: *MC500 Front Panel*

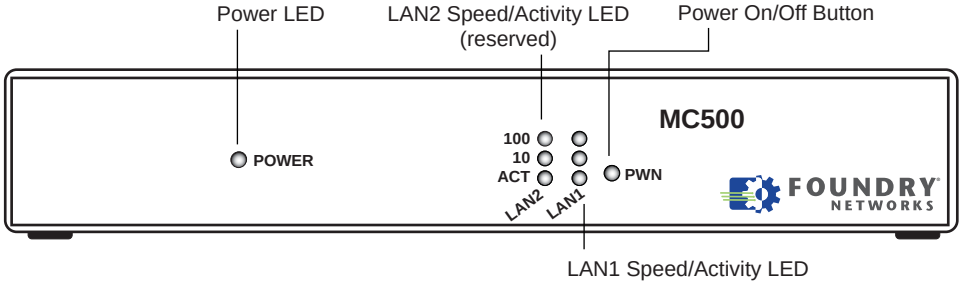


Figure 3: *MC1500 Rear Panel*

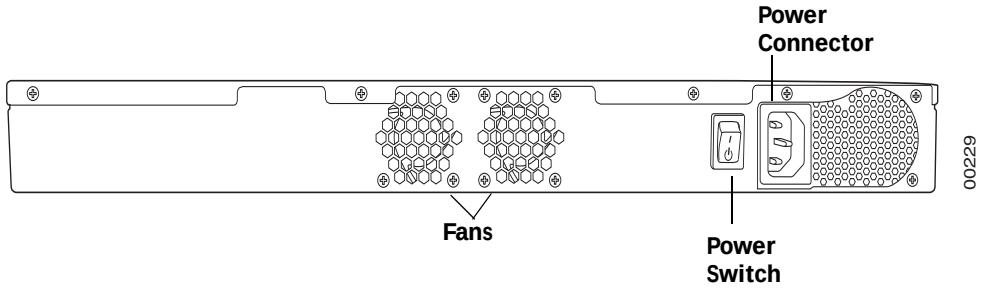
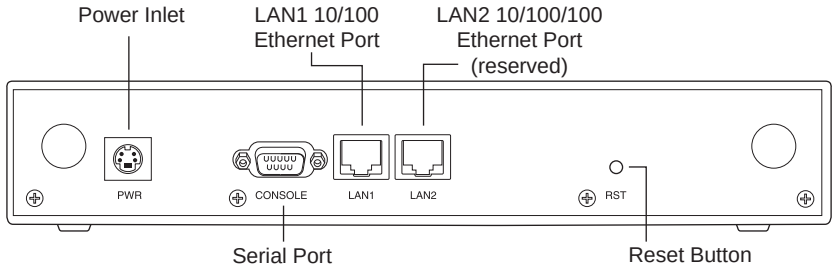


Figure 4: *MC500 Rear Panel*



Installing and Configuring MC1500

Installing and configuring the MC1500 for operation with Meru access points includes the following sections:

- *"Check Controller Package"* ***on page 20***
- *"Prepare for Installation"* ***on page 21***
- *"Install MC1500 Controller"* ***on page 22***
- *"Check Ethernet LED Status Indicators"* ***on page 22***

Check Controller Package

The controller package contains the following:

- Controller
- RJ-45 console cable (Note that this cable is different from the one used for other Fortinet controllers.)

- Power cable. The power cord provided is for use only with MC1500. It is not for use with any other Fortinet product or other brands of equipment.
- 2 Ethernet cables (only one is used)
- Mounting bracket kit (Note that these brackets are different from those used for other Fortinet controllers.)
- CD-ROM containing the System Director documentation

Prepare for Installation

Before you begin the installation, make sure you have the following:

Element	Requirement
WLAN equipment	• MC1500 controller (two, if installing a redundant configuration) • Up to 30 APs per controller
Ethernet switch	Layer 2 switches or a mix of Layer 3 and Layer 2 Gigabit switches with sufficient ports for the controller and all of the access points
Power over Ethernet	If power is not provided by the Ethernet switch, then PoE power injectors can be used between the switch and the access points.
Power	AC power outlets for both the switch and the controller.
Null modem cable	Serial cable with DB-9 female and RJ-45 connectors.
Ethernet cabling	CAT5 Ethernet cable.
Administration console	• Serial terminal running at 115200 baud, 8 bits, no parity, and 1 stop bit (115200 8N1). • After initial configuration, the SSH (Secure Shell) protocol or telnet can be used to communicate with the controller.
Controller IP settings	IP configuration settings for the controller (static or dynamic IP address and netmask, gateway server)
RADIUS server (optional)	IP address and passphrase for a RADIUS server providing 802.1X security.

Install MC1500 Controller

The form factor for the MC1500 is a 1U chassis designed for a 19" rack. Airflow enters from the front chassis and exits through the back, so ensure that there are no obstructions around the controller chassis that could reduce or block airflow.

To install the controller:

1. If you opt to install the controller in a rack, choose a location in the rack that accepts the clearance for a 1U high chassis. Insert the chassis into the chosen rack location and mount the unit with the provided rack mount kit.
2. Make a ground connection.
3. Set up a connection from a PC or laptop to the MC1500 Controller using the Console port and the cable provided.
4. On the PC or laptop, set up an ANSI or VT100 compatible terminal session with the following settings:
   - 115200 baud
   - 8 bits
   - no parity
   - 1 stop bit
   - no flow control

   If the terminal session does not appear on the computer, toggle the flow control.
5. Connect the provided power cord to the chassis and a wall outlet. The MC1500 powers up automatically when the power cord is plugged in and, unlike other controllers, beeps only once at power up.
6. Press the MC1500 power button to turn the unit off and then back on; you should see the bootup sequence start on your computer. Wait until bootup completes.
7. From the terminal session, initiate the **setup** command (login and password are both **admin**), as described in the “Performing an Initial Setup” section of the ***Meru System Director Getting Started Guide***.

Perform controller configuration and ESS configuration, as described in the remaining sections of the ***Meru System Director Getting Started Guide***. Once the unit is operating, the LEDs described in the next section are active.

Check Ethernet LED Status Indicators

The RJ-45 connector provides information about the Ethernet connection.

Figure 5: *RJ-45 Status Indicators*

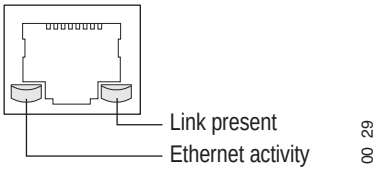


TABLE 1: *Ethernet Status Information*

LED	Activity	Description
Link Present	Green solid	Network connection
	Green blinking	Network activity
Ethernet Activity	Off	10 Mbps
	Green	100 Mbps
	Yellow	1000 Mbps

MC1500 LED Status Indicators

Monitor the status of the controller and the Ethernet connection using the various LED status indicators, located on the front of the chassis.

Controller LED Status Indicators

The controller status indicator LEDs are located on the front of the chassis, as shown *Figure 1 on **page 19***. The description of the LED states are shown in the following tables:

TABLE 2: *MC1500 LED Status Information*

LED	Color	Description
Power	unlit green solid	Unit is off Unit is on, power is good
Status	----------not used----------	
HDD	unlit amber flashing	This LED flashes amber when flash is accessed. It flashes during bootup, shutdown, login, and configuration checks.

Troubleshooting Beep Code Errors

If MC1500 beeps after bootup, it indicates an error. See the table below for details.

# of beeps	Description	Troubleshooting Action
1	Memory refresh timer error	Reseat the memory or replace the memory with known good memory.
3	Base memory read/write test error	Reseat the memory or replace the memory with known good memory.
6	8042 Gate A20 test error (unit cannot switch to protected mode)	Fatal error. Contact Fortinet support.
7	General exception error (processor exception interrupt error))	Fatal error. Contact Fortinet support.
8	Display memory error (system video adapter)	Video adapter failure. Contact Fortinet support.

Powering Off the Controller

Should it become necessary to power off the controller, use the CLI command **poweroff controller** before switching the controller off with the Power On/Off switch. The command grace-

fully brings the controller down to a state where power can safely be removed using the power switch.

	Failure to use the poweroff controller command before removing power from the controller can cause Flash card corruption and result in the controller becoming non-operational.

The green power LED is lit if power is supplied and off if there is no power.

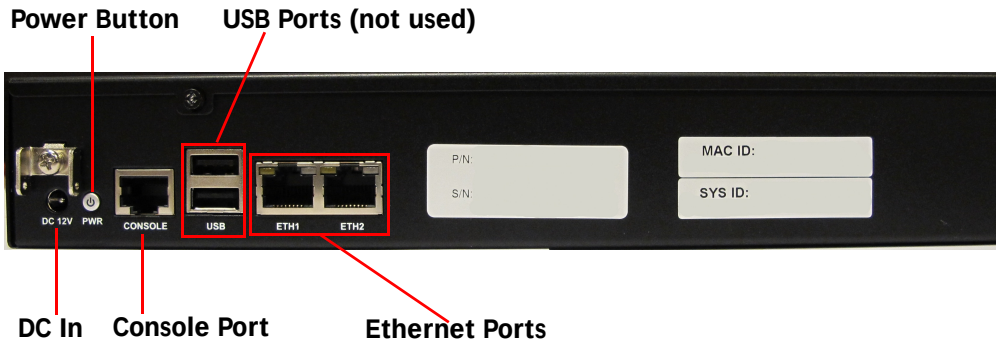
4 MC1550 Controller

The MC1550 is designed for small to medium-scale site deployments, such as small offices or remote branch sites. It supports customers requiring Layer 1-4 security, Fast Ethernet, and affordable performance. The MC1550 can support up to 50 APs.

The front and back of the MC1550 are shown below.

Figure 6: *MC1550 Front Panel*

Figure 7: *MC1550 Rear Panel*



Installing and Configuring MC1550

Installing and configuring the MC1550 for operation with Meru access points includes the following sections:

- *"Check Controller Package"* ***on page 28***

- *“Prepare for Installation”* ***on page 28***
- *“Install MC1550 Controller”* ***on page 29***
- *“Check Ethernet LED Status Indicators”* ***on page 30***

Check Controller Package

The controller package contains the following:

- Controller
- RJ-45 console cable (Note that this cable is different from the one used for other Fortinet controllers.)
- AC to DC adapter. This is for use only with MC1550. It is not for use with any other Fortinet product or other brands of equipment.
  - AC input 100-240V, 50-60Hz, 1.3A
  - DC input 12V, 3.75A (45W max)
- 2 Ethernet cables
- Rack mount attachments (for installing the controller in a standard 1U rack)
- CD-ROM containing the System Director documentation

Prepare for Installation

Before you begin the installation, make sure you have the following:

Element	Requirement
WLAN equipment	MC1550 controller (two, if installing a redundant configuration) Up to 50 APs per controller
Ethernet switch	Layer 2 switches or a mix of Layer 3 and Layer 2 Gigabit switches with sufficient ports for the controller and all of the access points
Power over Ethernet	If power is not provided by the Ethernet switch, then PoE power injectors can be used between the switch and the access points.
Power	AC power outlets for both the switch and the controller.
Null modem cable	Serial cable with DB-9 female and RJ-45 connectors.
Ethernet cabling	CAT5 Ethernet cable.

Element	Requirement
Administration console	Serial terminal running at 115200 baud, 8 bits, no parity, and 1 stop bit (115200 8N1). After initial configuration, the SSH (Secure Shell) protocol or telnet can be used to communicate with the controller.
Controller IP settings	IP configuration settings for the controller (static or dynamic IP address and netmask, gateway server)
RADIUS server (optional)	IP address and passphrase for a RADIUS server providing 802.1X security.

Install MC1550 Controller

The form factor for the MC1550 is a 1U chassis designed for a 19" rack when the rack-mounting brackets are attached. Airflow enters from the front chassis and exits through the back, so ensure that there are no obstructions around the controller chassis that could reduce or block airflow.

To install the controller:

1. If you opt to install the controller in a rack, choose a location in the rack that accepts the clearance for a 1U high chassis. Insert the chassis into the chosen rack location and mount the unit with the provided rack mount kit.
2. Make a ground connection.
3. Set up a connection from a PC or laptop to the MC1550 Controller using the Console port and the cable provided.
4. On the PC or laptop, set up an ANSI or VT100 compatible terminal session with the following settings:
   - 115200 baud
   - 8 bits
   - no parity
   - 1 stop bit
   - no flow control

   If the terminal session does not appear on the computer, toggle the flow control.
5. Connect the provided power cord to the chassis and a wall outlet. The MC1550 powers up automatically when the power cord is plugged in.
6. Press the MC1550 power button to turn the unit off and then back on; you should see the bootup sequence start on your computer. Wait until bootup completes.

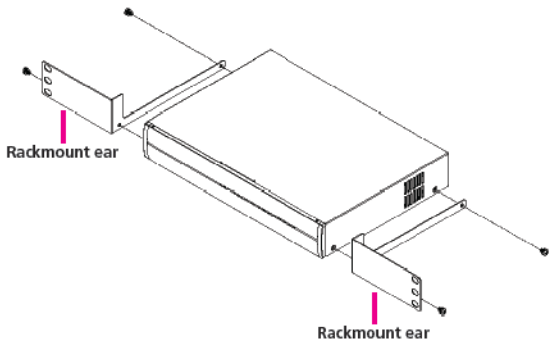
7. From the terminal session, initiate the **setup** command (login and password are both **admin**), as described in the “Performing an Initial Setup” section of the ***Meru System Director Getting Started Guide***.

Perform controller configuration and ESS configuration, as described in the remaining sections of the ***Meru System Director Getting Started Guide***. Once the unit is operating, the LEDs described in the next section are active.

Installing the Controller in a Rack

The MC1550 package contains two attachments designed to attach to the controller and allow it to be mounted in a standard 1U rack. Follow the instructions below:

1. Place the controller on a flat surface.
2. Align the two ears as indicated in the figure below and attach them using the screws as shown.



3. After tightening the screws, mount the controller in the rack using the appropriate rack screws.

Check Ethernet LED Status Indicators

The RJ-45 connector provides information about the Ethernet connection.

Figure 8: *RJ-45 Status Indicators*

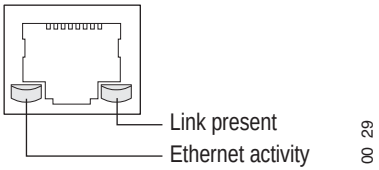


TABLE 3: *Ethernet Status Information*

LED	Activity	Description
Link Present	Green solid	Network connection
	Green blinking	Network activity
Ethernet Activity	Off	10 Mbps
	Green	100 Mbps
	Yellow	1000 Mbps

MC1550 LED Status Indicators

Monitor the status of the controller and the Ethernet connection using the various LED status indicators, located on the front of the chassis.

Controller LED Status Indicators

The controller provides several LED status indicators: two on the front (as shown in *Figure 6 on **page 27***) and one power indicator on the rear. The description of the LED states are shown in the following table.

TABLE 4: *MC1550 LED Status Information*

LED	Color	Description
Power (front)	Unlit Blue (solid)	Unit is off Unit is on, power is good
Power (rear)	Unlit Red (solid) Blue (solid)	No power supplied AC power is applied but DC power is down DC power is applied
Status	Unlit Blue (blinking)	No activity Read/Write activity on hard drive or flash

Powering Off the Controller

Should it become necessary to power off the controller, use the CLI command **poweroff controller** before switching the controller off with the Power On/Off switch. The command gracefully brings the controller down to a state where power can safely be removed using the power switch.

Failure to use the poweroff controller command before removing power from the controller can cause Flash card corruption and result in the controller becoming non-operational.

The blue power LED is lit if power is supplied and off if there is no power.

5 MC3200 and 4200 Controller

This guide describes how to physically install the MC3200 and MC4200 controllers for operation, and includes the following sections:

Controller Features

The MC3200 has the following capabilities:

Feature	Description
Network Interface	4 10/100/1000 Base-T Ethernet ports
USB connectors	2 front-mounted
Mounting requirement	1U rack
Cable provided	DB9 to RJ45 serial console cable
Maximum APs	200
Maximum Clients	2000
Maximum Throughput	2Gbps

The MC4200 has the following capabilities:

Feature	Description
Network Interface	4 10/100/1000 Base-T Ethernet ports Note: The MC4200 supports an optional 10Gbps module that can be purchased separately with a special license.
USB connectors	2 front-mounted
Mounting requirement	1U rack
Cable provided	DB9 to RJ45 serial console cable
Maximum APs	500
Maximum Clients	5000
Maximum Throughput	Standard: 4Gbps With 10Gbps module: 10Gbps

The 1G Ethernet ports support both Single Bonding and Dual Bonding mode (although bonding is not required for them to be functional). Note that if bonding is used, the bonding configuration must be identical in both the Network Manager and virtual controller interfaces.

Single Bonding—Allows all four ports to be bound and used as a single port.

Dual Bonding—Allows two ports at a time to be bound and used as dual ports.

See the illustrations below for physical details of the controller.

Figure 9: *MC3200/4200 (Front view)*

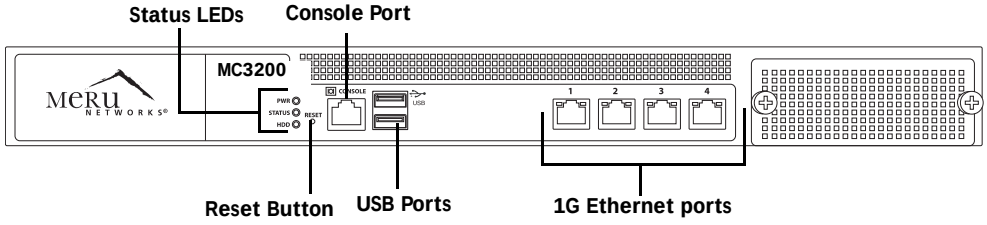
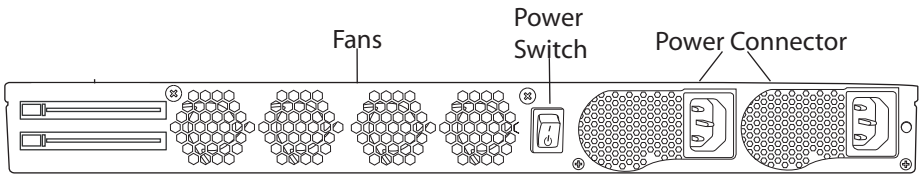


Figure 10: *MC4200 (Back view)*



The MC3200 only has a single power connection in the back.

The MC3200/4200 contains a lithium battery. There exists the risk of an explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Controller Package

Included in the Box

The MC3200/4200 package contains the following in addition to this guide:

- Controller with application software installed
- Two Ethernet cables (you will use only one of them)
- Documentation disk for the application loaded on the Services Appliance
- Console cable
- Two power cables (MC3200 has a single power cable)
- Rack mounting ears with 6 screws
- Four rubber feet
- Entitlement Certificate for licensing

You Also Need

- A computer with either Windows Internet Explorer or Mozilla Firefox, and a serial terminal program, running at 115200 baud, 8 bits, no parity, and 1 stop bit (115200 8N1)
- At least one powered AP accessible via the network (plugged into the test switch works well)

- Phillips head screwdriver
- Serial adapter for your laptop (if the laptop doesn't have a serial connection)
- Ethernet switch and cable
- Two (2) AC power outlets

Prepare for Installation

Before you begin the installation, make sure you have the following:

Element	Requirement
WLAN equipment	Controller (two, if installing a redundant configuration) At least one powered AP that can be accessed by the controller
Ethernet switch	Layer 2 switches or a mix of Layer 3 and Layer 2 Gigabit switches with sufficient ports for the controller and all of the access points
Power over Ethernet	If power is not provided by the Ethernet switch, then PoE power injectors can be used between the switch and the access points.
Power	AC power outlets for both the switch and the controller.
Null modem cable	Cable with DB-9 female and RJ-45 connectors.
Ethernet cabling	CAT5 Ethernet cable.
Administration console	Serial terminal running at 115200 baud, 8 bits, no parity, and 1 stop bit (115200 8N1). After initial configuration, the SSH (Secure Shell) protocol or telnet can be used to communicate with the controller.
Controller IP settings	IP configuration settings for the controller (static or dynamic IP address and netmask, gateway server)
RADIUS server (optional)	IP address and passphrase for a RADIUS server providing 802.1X security.

Install the Controller

The form factor for the MC3200/4200 is a 1U chassis designed for a 19" rack. Airflow enters from the front chassis and exits through the back, so ensure that there are no obstructions around the controller chassis that could reduce or block airflow.

To install the controller:

1. If you opt to install the controller in a rack, choose a location in the rack that accepts the clearance for a 1U high chassis. Insert the chassis into the chosen rack location and mount the unit with the provided rack mount kit.
2. Connect an ethernet cable to the controller and the test switch.
3. Set up a connection from a PC or laptop to the Controller using the Console port and the cable provided.
4. On the PC or laptop, set up an ANSI or VT100 compatible terminal session with the following settings:
   - 115200 baud
   - 8 bits
   - no parity
   - 1 stop bit
   - no flow control

   If the terminal session does not appear on the computer, toggle the flow control.
5. Connect the provided power cord(s) to the chassis and a wall outlet. The controller powers up automatically when the power cord is plugged in and, unlike other controllers, beeps only once at power up.

The MC4200 requires two power cables for standard operation. If one cable is used, an alarm will sound at bootup. This alarm can be silenced by pressing the red button on the back of the controller.

6. From the terminal session, initiate the **setup** command (login and password are both **admin**), as described in the “Performing an Initial Setup” section of the ***Meru System Director Getting Started Guide***.

Perform controller configuration and ESS configuration, as described in the remaining sections of the ***Meru System Director Getting Started Guide***. Once the unit is operating, the LEDs described in the next sections are active.

Check Ethernet LED Status Indicators

The RJ-45 connector provides information about the Ethernet connection.

Figure 11: *RJ-45 Status Indicators*

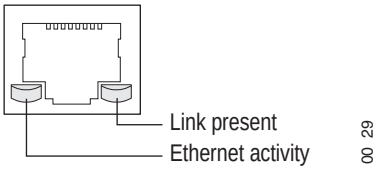


TABLE 5: *Ethernet Status Information*

LED	Activity	Description
Link Present	Green solid	Network connection
	Green blinking	Network activity
Ethernet Activity	Off	10 Mbps
	Green	100 Mbps
	Yellow	1000 Mbps

Installing the 10G Module (MC4200 Only)

The 10G module requires an SFP+ module (purchased separately) and the appropriate fiber optic cable to be installed prior to installing the module.

The MC4200 controller model allows users to install an upgrade network module that allows for throughput of up to 10Gbps. This requires a 10G Module license as well as the physical module itself. Follow the instructions below in order to properly install the module.

The standard 10/100/1000 ethernet ports installed in the controller by default are not operational when the 10G module is installed.

1. Prior to connecting the module, you must install the required add on license.
   a) Open an Internet browser and navigate to http://www.merunetworks.com/support/.
   b) Login to your Fortinet Support account using the **Login** link (if you do not have an account already, click **Register** to obtain credentials).
   c) From the Licensing section, click **Activate your Licenses**.

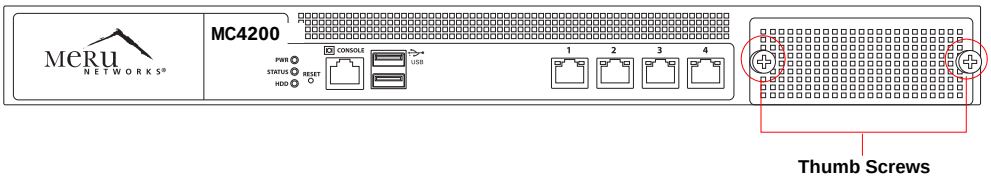
d) Enter the license information provided by your entitlement certificate or email and download the license to your local machine.

e) Access the controller's web UI and click **Maintenance>Add License**.

f) Browse to the license saved in Step d above and click **Import License**.

2. Save the active running configuration and shut down the controller.
3. Unscrew the two thumb screws on the front of the controller, as indicated in *Figure 12 on **page 39***.

Figure 12: *10G Card Expansion Slot*



4. Remove the small screw on the underside of the controller locking the expansion slot cover in place.
5. Slide the slot cover off of the controller.
6. Insert the 10G module into the slot on the front of the controller and reconnect all the screws.
7. Connect the fiber optic cable to the first 10Gb port and restart the machine.
8. After bootup has finished, access the controller's CLI and use the following commands to enable the module:

```
default(15)# configure terminal
default(15)(config)# 10gig-module enable
```

If prompted to configure bonding at this point, configure it to none in order to ensure optimal functionality of the 10G module.

9. Connect the module to the 10Gb port on the network switch (if this has not already been done).
10. Save the running configuration again and reboot the controller.

Controller LED Status Indicators

Monitor the status of the controller and the Ethernet connection using the various LED status indicators, located on the front of the chassis. The controller status indicator LEDs are located on the front of the chassis, as shown *Figure 9 on **page 34***. The description of the LED states are shown in the following tables.

TABLE 6: *MC3200/4200 LED Status Information*

LED	Color	Description
Power	unlit green solid	Unit is off Unit is on, power is good
Status	----------not used----------	
HDD	unlit amber flashing	This LED flashes amber when flash is accessed. It flashes during bootup, shutdown, login, and configuration checks.

Powering Off the Controller

Should it become necessary to power off the controller, use the CLI command **poweroff controller** before switching the controller off with the Power On/Off switch. The command gracefully brings the controller down to a state where power can safely be removed using the power switch.

Failure to use the poweroff controller command before removing power from the controller can cause Flash card corruption and result in the controller becoming non-operational.

The green power LED is lit if power is supplied and off if there is no power.

6 MC5000 Chassis Controller

The MC5000 Controller Chassis is a multi-slot enclosure that holds up to five independently functioning MC5000 Controller blades. The MC5000 Controller Chassis is a scalable solution well suited for large-scale deployments. As it is completely modular, controller blades can be added as the site requires.

The MC5000 Controller Chassis includes one shelf manager card, one power supply, and two fan trays. An additional shelf manager card and power supply are available as options that can be added for redundancy. The MC5000 blade can also be upgraded with the AMC accelerator module to increase the Ethernet port count to 4, and performance to 4 GBps line rate.

Each MC5000 Controller blade in the chassis is configured and operates as a fully-functional, stand-alone controller running System Director. Each controller blade must be configured with a separate management IP address, as performed in the **setup** procedure in the ***Meru System Director Getting Started Guide***. Dual Ethernet port functionality is supported if the second port is configured, as described in the Dual Ethernet feature in System Director documentation.

The MC5000 Controller Chassis is well suited for redundant controller configurations using either the standard N+1 feature (with 1 master and 1 backup controller) or the optional N+1 Redundant Controller feature (one slave controller for up to four master controllers).

The MC5000 Controller Chassis supports:

- A maximum of five MC5000 Controller blades
- Each MC5000 Controller blade supports a maximum of 200 APs, and with the optional accelerator module, a maximum of 300 APs.
- Complete support of System Director standard and optional features such as N+1 Redundant Controller, Dual-Ethernet, Per-User Firewall, and so forth.
- Controllers can be configured and managed using the System Director Web UI.

Figure 13: *MC5000 Chassis Components (Front View)*

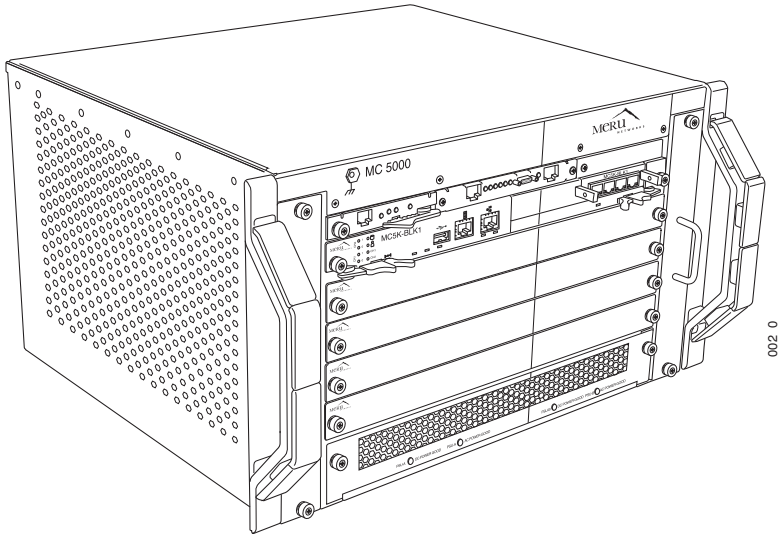
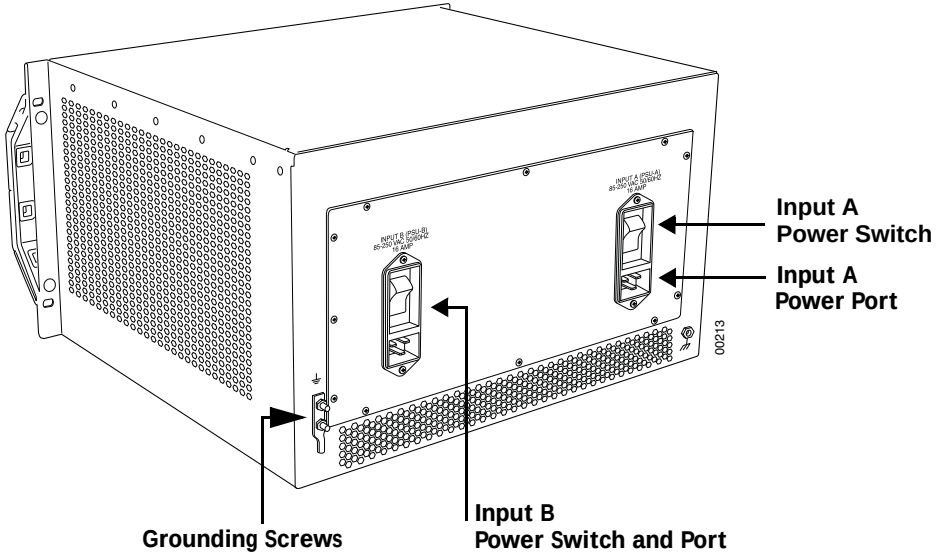


Figure 14: *MC5000 (back view)*



Installing and Configuring MC5000

This section describes how to install, configure, and maintain the MC5000 Chassis Controller for operation with access points, and includes the following sections:

Prepare for Installation

Before you begin the installation, make sure you have the following:

Element	Requirement
WLAN equipment	• One MC5000 Controller Chassis • One to five MC5000 Controller Blades • The required number of APs
Ethernet switch	Layer 2 switches or a mix of Layer 3 and Layer 2 100/1000BaseT switches with sufficient ports for the controllers and access points
Power over Ethernet	Each access point must have access to 802.3af-compliant Power over Ethernet (PoE). If this is not provided by the switch, then PoE power injectors can be used between the switch and the access points.
Power	AC power for the switch and the controller.
Null modem cable	RJ-45 cable
Ethernet cabling	CAT5 Ethernet cable.

Element	Requirement
Administration console	• Serial terminal running at 115200 baud, 8 bits, no parity, and 1 stop bit (115200 8N1). • After initial configuration, the SSH2 (Secure Shell) protocol or telnet can be used to communicate with the controller.
Controller IP settings	IP configuration settings for the controller (static or dynamic IP address and netmask, gateway server)
RADIUS server (optional)	IP address and passphrase for a RADIUS server providing 802.1X security.

Install MC5000 Controller Chassis

Perform the procedures in the following sections to install and configure the MC5000 Controller Chassis.

The MC5000 Controller Chassis can be set on a flat surface or rack-mounted in a standard 19” telco rack.

The MC5000 Controller blades and Chassis frame are packaged separately. For the initial installation, use the following procedure:

1. Unpack the shipping containers and verify the following items are included:
   - MC5000 Chassis with installed Shelf Manager card(s), 2 fans, and power supply
   - Chassis power cord
   - Number of Controller blades that were ordered
   - Release 3.6 documentation CD
2. Install the MC5000 Chassis in a 19” standard rack, if so desired. The following must be considered when installing the chassis in a rack:
   - Elevated Operating Ambient Temperature—If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra) of 40oC (104oF).
   - Reduced Air Flow—Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
   - Mechanical Loading—Mounting of the equipment in the rack should be such that a hazardous condition is not created due to uneven mechanical loading.
   - Circuit Overloading—Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading circuits might have on over-

current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

- Reliable Earthing—Reliable earthing of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (such as using a power strip and so forth).

a) To install MC5000 Chassis in rack, move the MC5000 Chassis to the rack or cabinet where it will be installed. Remove any packing materials from the chassis.

Installing an MC5000 chassis is a 2-person task. The base chassis with filler panels weighs 50 pounds, and a fully loaded chassis weighs up to 75 pounds. At least 2 installers are required to do this task safely.

b) Lift the MC5000 Chassis into position and attach the chassis to the rack rails. Ensure that all mounting screws (both sides) are installed to secure the MC5000 Chassis to the mounting rails.

3. Attach a ground wire to the MC5000 Chassis and to a grounded location.
4. To install an MC5000 Controller blade:

a) To properly ground yourself, attach a grounding strap to the grounding plug on the front (top left corner) of the MC5000 Chassis.

b) For the slot where the MC5000 Controller blade will installed, remove the filler panel by unscrewing the panel screws. Store the filler panel in a safe place. Slots are numbered starting with 1 on the bottom and 5 on top (just below the Shelf Manager).

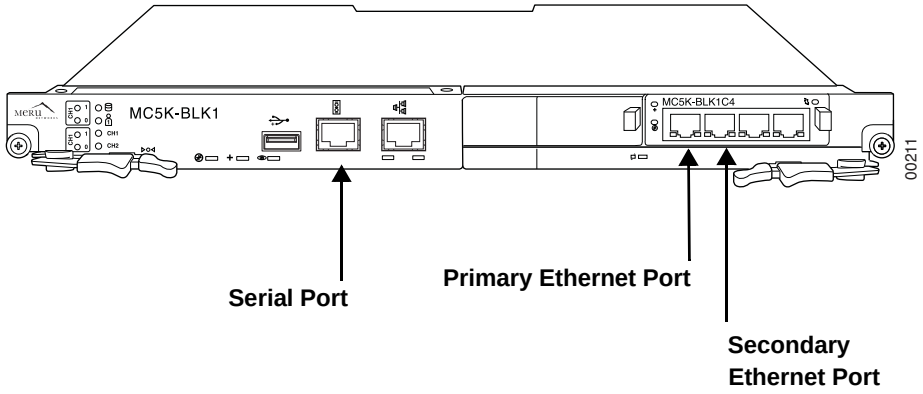
Electrostatic Discharge—The blades contain ESD-sensitive devices, and can be damaged if not handled in accordance with approved ESD guidelines. Do not remove any blade from its ESD packaging until you are ready to install it in the MC5000 chassis.

c) Insert the MC5000 Controller blade by following the directions *"MC5000 Controller Blade Insertion and Removal"* ***on page 58***.

Seating this blade properly can be tricky and the Controller will not boot if seated improperly. Be sure to look at the directions.

5. Connect the first Ethernet cable to the primary Ethernet port (the left-most Ethernet port) on the front of the MC5000 Controller blade and to a switch, as described in the System Director Getting Started Guide.
6. Configure the Switch settings for connection to MC5000 Controller Blade interfaces running N+1 and/or Dual Ethernet—Redundant mode to the following settings:
   - Spanning Tree link type = Point-to-point
   - MAC aging time for native VLAN of Controller = 10s
   - Forward delay timer for Controller VLAN = 4s
   - Port settings = Portfast

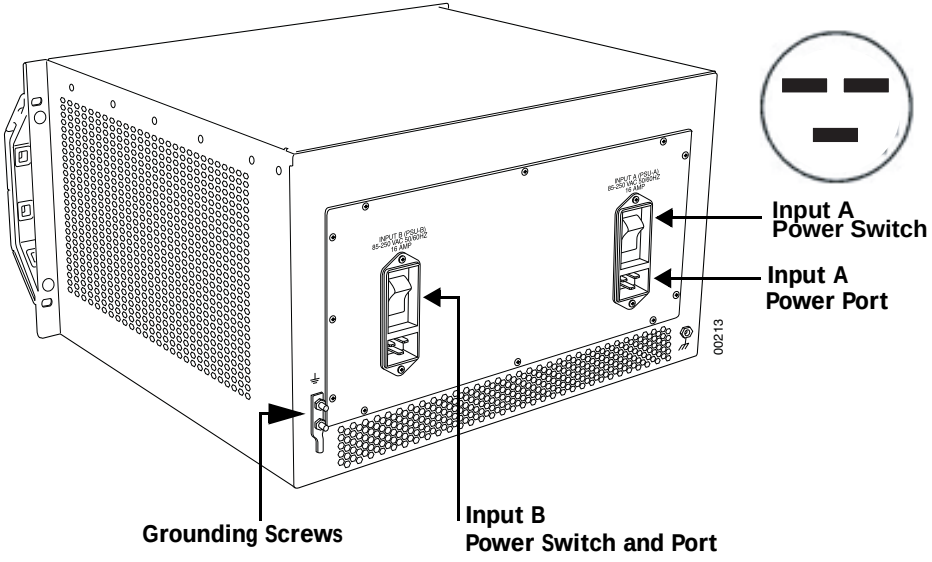
Figure 15: *MC5000 Controller Blade Ports*



If a secondary Ethernet connection is required, connect it to the Secondary Ethernet port indicated in the figure above. The Ethernet connections on the MC5000 Controller blades can be configured to the same subnet or different subnets, depending on the type of network configuration that is required.

7. Connect the power cord to the Input A Power Port on back of the chassis and to the wall AC power source. (Input B is the optional power supply, if it has been purchased.)The MC5000 WLAN controller has two power supplies. Each power supply has a non-locking 20A 125/230VAC power receptacle with an IEC-320 C19 connector.

Figure 16: *MC5000 Chassis (Rear View)*



8. Power up the chassis by flipping the Input A On/Off switch on the back of the chassis to On. Ensure that the fans are running, and cool air is flowing through the chassis.
9. Press the power switch to the On position.

   The Power On System Test runs and completes with one of the following codes, depending on the system status.

TABLE 7: *MC5000 Controller Blade POST Results*

Element	Requirement
1 Short beep	Normal POST, controller status is normal
2 Short beeps	CMOS error
One long and one short beep	DRAM error
One long and two short beeps	Video (Mono/CGA Display Circuitry) issue
One long and three short beeps	Keyboard/Keyboard card error
One long and nine short beeps	ROM error
Continuous long beep	DRAM problem
Repeating short beeps	There are some problem with the Power source

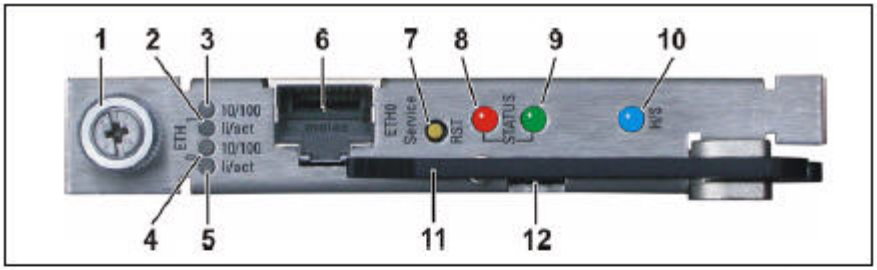
10. Set up a serial connection from a PC or laptop to the MC5000 Controller blade. For the initial controller configuration, you must connect to the MC5000 Controller blade using the Serial port.
    - On the PC or laptop, set up an ANSI or VT100 compatible terminal session with the following settings:
    - 115200 baud
    - 8 bits
    - no parity
    - 1 stop bit
    - no flow control
11. From the console, initiate the setup command (login and password are both admin), as described in the “Performing an Initial Setup” section of the System Director Getting Started Guide.
12. Perform controller configuration and ESS configuration, as described in the remaining sections of the System Director Getting Started Guide.

About the Shelf Manager

The Shelf Manager monitors the power, cooling and operation of the chassis. Status is visible via the LEDs located on the shelf manager blade and on the Shelf Alarm Panel, located in the center of the Shelf Manager blade. Additionally, fault and error messages can be sent to an SNMP network manager using the Shelf Manager Ethernet port, configurable via the CLI or Web UI.

The Shelf Manager LED location and status are shown in the following figure. The green LED, shown in location 9 in the following figure, displays with normal operation.

Figure 17: *Shelf Manager Status LED Location and Description*



1	Fixing screw	7	RESET push button
2	ETH 1 Link/Activity LED (green) - On = Link - Off = No Link - Blinking = Activity	8	Shelf Manager Status LED (red) - Red = Out of Service
3	ETH 1 Speed LED (yellow) - Off = 10 Mb - On = 100 Mb	9	Shelf Manager Status LED (green) - Solid Green = in Service, active Shelf Manager - Blinking = in Service, Backup Shelf Manager
4	ETH 0 Speed LED (yellow) - Off = 10 Mb - On = 100 Mb	10	Hot Swap LED (blue) - Solid Blue = ready to remove - Blinking = Hot Swap is requested - Off = No Hot Swap possible
5	ETH 0 Link/Activity LED (green) - On = Link - Off = No Link - Blinking = Activity	11	Extraction handle
6	ETH 0 Ethernet Service Connector (RJ45)	12	Hot Swap switch - Hot Swap is activated by lifting the extraction handle. (See next chapter)

Checking the Shelf Manager Alarm Panel LEDs

The LEDs on the Shelf Manager Alarm Panel convey the status of the chassis alarms. Each sensor monitored by the shelf manager has four defined operating ranges: normal , minor alarm, major alarm, and critical alarm. When any one of the sensors deviates from normal, one of the three alarm LEDs lights.

User alarms are currently neither used nor defined.

Figure 18: *Shelf Manager Alarm Panel LEDs*

For example, a power supply voltage may have a normal operating range to 4.9 to 5.1V. Then, depending on how far out of range the current reading is, the appropriate alarm is raised. To find out which sensor indicated a problem, gather the following information and then contact Fortinet support. The easiest way is to capture this is to output to a file as you type the commands. Type the commands from the Unix prompts, not from the Shelf Manager CLI.

- Dump SEL With Details: clia sel -v
- Display Management Processor Details: clia ipmc -v
- Display Sensors Outside of Normal Thresholds: clia sensordata -t
- Display the sensor values: clia sensordata
- Display Installed Firmware for Both Parts of Shelf Manager Flash Memory: version
- Display Chassis FRU Data for Chassis and Shelf Managers:
  - clia fruinfo -v 10 0
  - clia fruinfo -v 12 0
  - clia fruinfo -v 20 1
  - clia fruinfo -v 20 2
- Display Linux System Messages File: cat /var/log/messages
- Display Linux Boot Messages: dmesg

Using the information from these logs, a support person can tell you which sensor triggered the alarm and how to reset the alarm after you fix the problem. Note that critical alarms can only be reset by removing and then reseating the blade.

Serial and Alarm Card Relays

The incoming signals for the alarm board are SELV and are not more than 30V dc/1A the rating for the contact.

For more information about Shelf Manager, see the Shelf Manager User Guide.

Powering Off the Controller

Should it become necessary to power off the controller, it is recommended you use the CLI command poweroff controller before switching the controller off with the Power On/Off switch.

The command gracefully brings the controller down to a state where power can safely be removed using the power switch.

Failure to use the poweroff controller command before removing power from the controller can cause Flash card corruption and result in the controller becoming non-operational.

LED Status Indicators

Monitor the status of the controller and the Ethernet connection using the various LED status indicators, located on the front of the chassis.

Controller LED Status Indicators

The controller status indicator LEDs are located on the front of the chassis, as shown in the figures in the previous chapter. The description of the LED states are shown in the following tables.

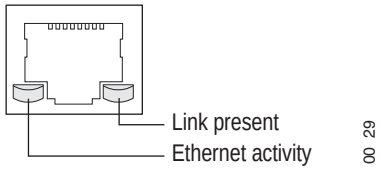
TABLE 8: *MC5000 LED Status Information*

LED	Color	Description
Power	Amber Solid Unlit	Powered on Powered off
Status	Unlit Green	Unimplemented Unimplemented
G1 10/100/1000	Unlit Green solid Amber solid	LAN Speed 10 Mbps LAN Speed 100 Mbps LAN Speed 1000 Mbps
Link/Act	Unlit Green solid Green blinking	Link Down/ No Activity Link Up Rx/Tx Activity

Ethernet LED Status Indicators

The RJ-45 connector provides information about the Ethernet connection.

Figure 19: *RJ-45 Status Indicators*



LED	Activity	Description
Link Present	Green solid	Network connection
	Green blinking	Network activity
Ethernet Activity	Off	10 Mbps
	Green	100 Mbps
	Yellow	1000 Mbps

Installing the MC5000 Accelerator Card

If your accelerator card was shipped with an MC5000 blade, the card is already installed in the blade. You don't need to do any installation; stop now. In this case, System Director 3.6 is already on the MC5000; you do not have to upgrade System Director on the MC5000. If you are adding an accelerator card to an existing MC5000, first upgrade your MC500 to system director 3.6.

Your MC5000 using the Accelerator Card must be running System Director 3.6 because only this version of System Director supports the Accelerator Card.

When a multimode Accelerator Card is installed into an existing MC5000 blade, the blade's user capacity increases from 2000 to 3000 stations and also increases throughput speed from 1G to 4G (with all 4 ports aggregated). Instead of 200 APs, 300 APs are supported. Although there are two slots in a blade, only one (either one) can be used at a time with the second slots are reserved for future use.

To use the Accelerator Card, you also need either 1G copper or LC fiber SFP connectors for the connections; the card cannot operate without these SFP connectors. These are standard connectors and are not sold through Fortinet. The fiber module supports SFP (Small Form-Factor Pluggable) GBIC Modules and works with Nortel, 3Com, and Cisco SFP GBIC. The SFP ports support both Single Mode (SM) and Multi-mode (MM) fiber.

You can mix copper and fiber SFP connectors on one Accelerator Card. Because the connectors are optional, the appropriate connecting cables will vary.

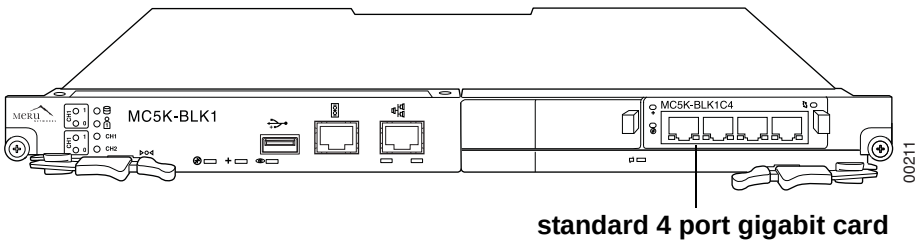
To install the Accelerator Card, follow these steps:

1. If your MC5000 is not running System Director 3.6 or later, upgrade it following the directions in any System Director release note.
2. Remove the blade from the MC5000. The blade is hot-swappable but the accelerator card is not.

Do not swap accelerator cards in an active blade; this can cause damage to the blade.

3. Insert the SFPs into any or all of the four slots.
4. Remove the existing card from an MC5000 blade as indicated in *Figure 20 on* ***page 53***.

Figure 20: *MC5000 Blade*



5. Insert the Accelerator Card into the slot until it is seated.
6. Turn on the MC5000.

Increasing Bandwidth with Port Bonding

Port bonding can be configured both MC4100 and the MC5000 Accelerator Module.

On the MC5000 the wireless controller blade part# MC5K-BLK1C4 with 4 port copper does not support bonding. Only the blade MC5K-BLK1A4 or the MC5K-BLK1C4 with the optional MC5K-AM5040 supports port bonding.

To increase bandwidth on one or both ports used, configure port bonding, also sometimes called port aggregation. Do this in one of two possible configurations. You can either combine any or all of the four 1G ports into a single logical port or you can configure two ports, each with 2G, where G1-G2 are bonded together and G3-G4 are bonded together.

If a bonded controller sees its Ethernet interfaces/links as UP, it means that the switch is correctly configured for bonding, so the controller then starts pushing traffic through the ports based on these two criteria:

- Is single or dual mode is configured?
- How many controller Ethernet links are UP?

For example, you could have G1/G2/G3 enabled for single bonding, resulting in 3G throughput, while G4's link is not UP due to misconfiguration on the switch or because no Ethernet cable is present. Look at *Figure 21 on* ***page 55*** and *Figure 22 on* ***page 56*** for more details on cabling.

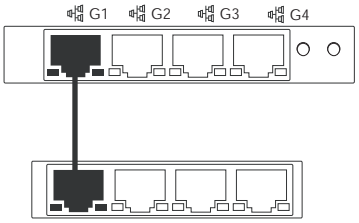
Configure port bonding from the CLI with the configuration commands bonding single or bonding dual. Check on a controller's bonding (single or dual) with the command show controller.

Configure port bonding from the GUI by clicking Configuration > Devices > Controller , selecting either an MC4100 or MC5000 with an accelerator module, and then setting Port Bonding to single (default) or dual.

Single Port Bonding

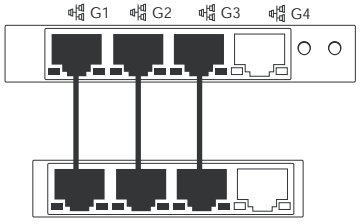
Bonding is single by default, where all ports are combined into one single port. You cannot separate traffic with single bonding. To do this, see *"Using Dual Bonding to Separate Traffic"* ***on page 57***. With single bonding, there are four different ways to cable to the switch - see *Figure 21 on* ***page 55***.

Figure 21: *Cabling Single Bonding to a Switch*



1 Gbps

Bond these 2 switch ports for 2G



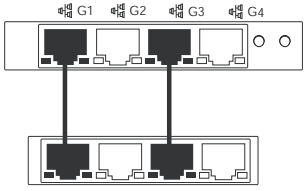
Bond these 3 switch ports for 3G

Bond these 4 switch ports for 4G

Dual Port Bonding

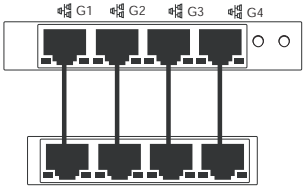
For dual port bonding, G1-G2 are bonded together and G3-G4 are bonded together. Dual bonding is used not only to increase bandwidth, but also to separate traffic. Dual bonding can be either a redundant or active configuration. In both cases, G3-G4 has its own IP address. There are three viable ways to cable a dual bonded controller to a switch and two ways that will not work - see *Figure 22 on* ***page 56***.

Figure 22: *Cabling Dual Bonding to a Switch*



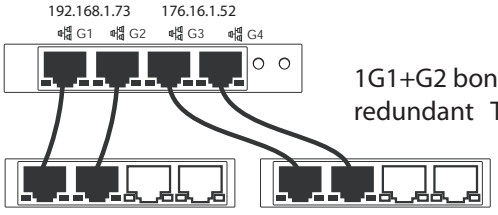
G1+G2 bonded & active G3+G4 bonded & active
One IP address

First 2 switch ports bonded, second 2 bonded



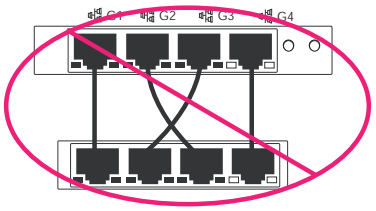
G1+G2 bonded & active G3+G4 bonded & active
Two IP addresses

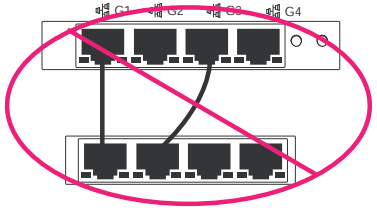
First 2 switch ports bonded, second 2 bonded



1G1+G2 bonded & active G3+G4 bonded & redundant Two IP addresses

Two switches, each with first 2 switch ports bonded





Don't do this using Layer 3! Using Layer 2, it works but is not a good practice.

Using Dual Bonding to Separate Traffic

When using single mode bonding, you cannot enable a second IP address on the controller. If you enable the G2 interface using single mode and provide it with an IP address, any/all bonding functionality on the controller is removed. The only bonding option that segregates traffic is dual mode. To achieve this, follow these steps:

1. Enable dual bonding and configure a redundant interface on the controller. This interface will be G2. This can be confusing because G1+G2 are combined and G3+G4 are combined so you could logically think that you would configure the interface G3. You are not.

   Enable bonding and configure the second (redundant) interface on the controller from the CLI with these commands:

   ```
   Redundant# configure terminal
   Redundant(config)# bonding dual
   Redundant(config)# interface FastEthernet 2
   Redundant(config-if-FastEth)# type redundant
   Redundant(config-if-FastEth)# end
   Redundant# copy running-config startup-config
   Redundant# reload controller
   Active# configure terminal
   Active(config)# bonding dual
   Active(config)# interface FastEthernet 2
   Active(config-if-FastEth)# type active
   Acitve(config-if-FastEth)# ip address 172.18.61.10 255.255.255.0 (OR) ip
   address dhcp
   Active(config-if-FastEth)# gw 172.18.61.1
   Active(config-if-FastEth)#end
   Active# copy running-config startup-config
   Active# reload controller
   ```
2. Connect an Ethernet cable to both the physical G1 port on the controller and the S1 port on the switch.
3. Connect an Ethernet cable to both the physical G2 port on the controller and the S2 port on the switch.
4. Connect an Ethernet cable to the physical G3 port on the controller (not G2 because dual bond means physical ports G3 and G4 are represented by logical port G2 as seen on the controller config). Connect the other end to the S3 switch port.
5. Connect an Ethernet cable to both the physical G4 port on the controller and the S4 port on the switch.

Now the controller has these settings:

- Physical ports G1 and G2 are logically referred to, and configured as, G1 on the controller. Any references in the GUI or CLI to G1 really means G1 + G2.
- Physical ports G3 and G4 are logically referred to, and configured as, G3 on the controller. Any references in the GUI or CLI to G3 really means G3 + G4.

Maintaining the MC5000 Chassis

The following tasks may be needed to maintain the MC5000 chassis:

MC5000 Controller Blade Insertion and Removal

To install an MC5000 Controller blade in the MC5000 Chassis:

1. Remove the filler panel of the slot. Store in a safe location.
2. Carefully align the PCB edges in the bottom and top card guides.
3. Insert the MC5000 Controller blade into the chassis until it makes contact with the backplane connectors.
4. Using both ejector handles, push the board into the backplane connectors until both ejectors latch into place. You should hear a click as the blade engages with the backplane, and the ejector handles should be parallel to the chassis.
5. Fasten screws next to the ejector handles.

Electrostatic Discharge—The blades contain ESD-sensitive devices, and can be damaged if not handled in accordance with approved ESD guidelines. Do not remove any blade from its ESD packaging until you are ready to install it in the MC5000 chassis.

To remove an MC5000 Controller blade:

1. Power down the controller using the poweroff controller command.
2. Unscrew the two ejector handle screws on the MC5000 Controller blade front panel.
3. Unlock both handle latches.
4. Wait until the blue LED is fully ON (not blinking); this means that the hot swap sequence is ready for the board removal.
5. Use both ejectors to disengage the MC5000 Controller blade from the backplane.
6. Pull the MC5000 Controller blade out of the chassis.
7. Replace the front panel slot.

Replacing the MC5000 Communications Module

An option is available for the MC5000 blade to increase Ethernet port count from 2 to 4 by replacing the standard communications module with the AMC acceleration module. The AMC acceleration module leverages the advanced features in System Director 3.6 such as Fastpath and port bonding to increase throughput and customize data delivery options. Port bond-

ing can be configured on the four Ethernet ports using the command bonding single (to combine all ports into a single logical port of 4G) or bonding dual (to configure two ports, each with 2G, where G1-G2 are bonded together and G3-G4 are bonded together). Logically, after bonding, the ports are the same as the current MC3000 where there are either 1 or 2 Ethernet ports for N+1. You can have a maximum of two IP addresses for the MC5000, even if you are not using channel bonding. Ports 1 and 3 can have separate IP addresses, as long as dual bonding (bonding dual) is configured (even if extra bandwidth provided by bonding is not needed).

Install the accelerator module by following these steps:

1. Power off the MC5000 blade by pushing the right side blade ejector tab to the left, towards the center of the blade.
2. This powers down the MC5000 blade.
3. Remove any Ethernet cables that are connected to the communications ports.
4. Grasp the black lever on the right side of the communications module and pull out to remove the module.
5. Locate the new module, and insert the module into the MC5000 blade, pushing in until the module is seated into the blade.
6. Push the blade right side ejector tab to the left to power on the blade.
7. Connect the Ethernet cables to the Ethernet ports.

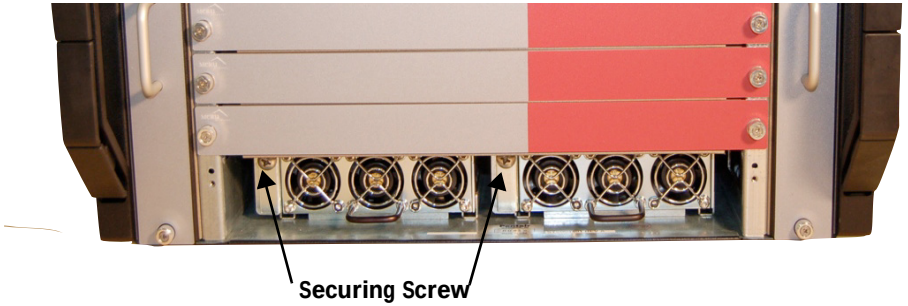
Replacing MC5000 Chassis Power Supplies

By default, one power supply is shipped in the MC5000 Chassis. An optional second power supply can be purchased.

To remove an MC5000 Chassis power supply:

1. Unscrew the two screws on the power supply grille panel on the MC5000 chassis front. This provides access to the power supply bay.

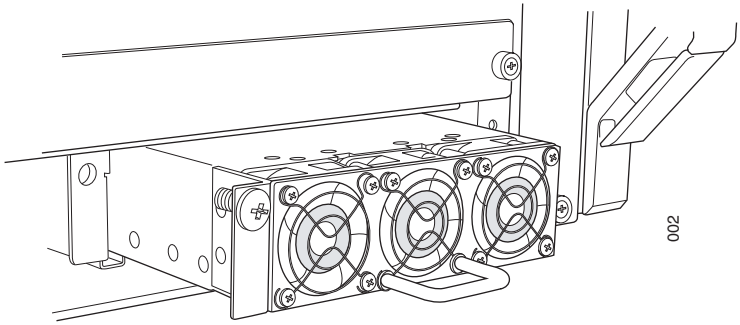
Figure 23: *wo Power Supplies within Power Supply Bay*



2. Using a #2 Phillips screwdriver, unscrew the securing screw in the upper left corner of the power supply front.

3. Grasping the power supply handle, pull the power supply out of the chassis.

Figure 24: *Partially Inserted Power Supply*



To replace an MC5000 Chassis power supply:

1. Push the replacement power supply into the chassis on the power supply guide rails.
2. Using a #2 Phillips screwdriver, secure the power supply to the chassis by tightening the securing screw on the power supply front.
3. Replace the power supply grille panel on the MC5000 chassis front. Retighten the two panel screws.

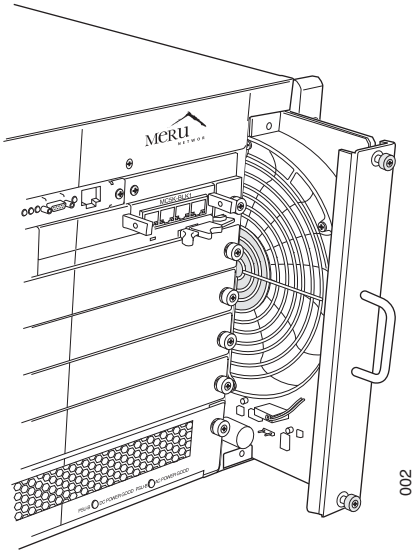
Replacing MC5000 Fans

To remove an MC5000 Chassis fan:

1. Unscrew the two screws on the fan panel top and bottom.
2. Using the handle, pull the fan out of the chassis.

Figure 25: *Partially Inserted Fan*

aa



To replace an MC5000 Chassis fan:

1. Push the fan into the chassis on the guide rails.
2. Secure the fan to the chassis by tightening the front panel top and bottom screws.

7 MC6000 Chassis Controller

The MC6000 Chassis is a multi-slot enclosure that holds up to ten independently functioning MC6000 Controller blades. This scalable solution is well suited for large-scale deployments—as it is completely modular, controller blades can be added as the site requires.

The MC6000 Chassis includes two power supply modules. Each MC6000 Controller blade in the chassis is configured and operates as a fully-functional, stand-alone controller running System Director. Each controller blade must be configured with a separate management IP address, as performed in the setup procedure in the System Director Getting Started Guide.

The MC6000 Chassis is well suited for redundant controller configurations using either the standard N+1 feature (with 1 master and 1 backup controller) or the optional N+1 Redundant Controller feature (one slave controller for up to four master controllers).

The MC6000 Chassis supports:

- A maximum of ten MC6000 Controller blades
- Each MC6000 Controller blade supports a maximum of 500 APs
- All blades provide 6 network connection ports
- Complete support of System Director standard and optional features such as N+1 Redundant Controller, Dual-Ethernet, Per-User Firewall, and so forth.
- Controllers can be configured and managed using the System Director Web UI.

Figure 26: *MC6000 Chassis Components (Front View)*

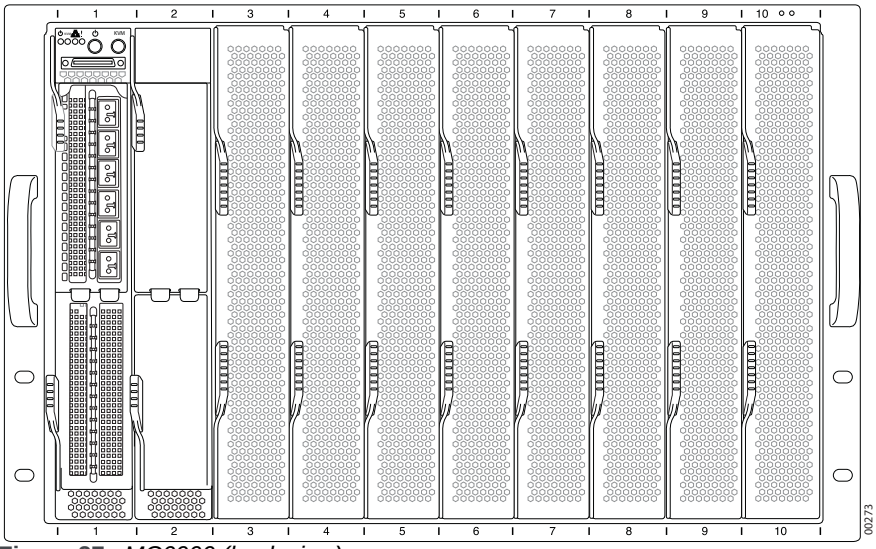
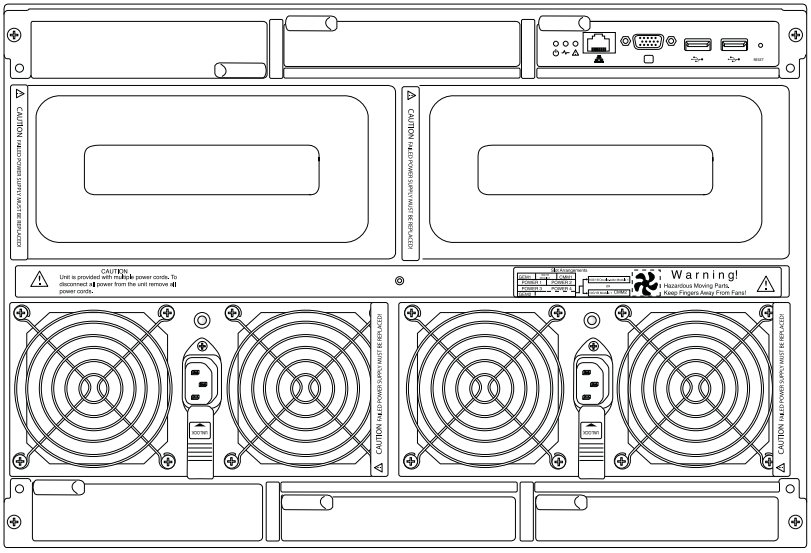


Figure 27: *MC6000 (back view)*



The 10-port 1Gb switch module located on the back of the chassis is not currently used.

Installing and Configuring MC6000 Chassis

This section describes how to install, configure, and maintain the MC6000 Chassis Controller for operation with access points, and includes the following sections:

Prepare for Installation

Before you begin the installation, make sure you have the following:

Element	Requirement
WLAN equipment	• One MC6000 Controller Chassis • MC6000 Controller Blade(s) • APs
Ethernet switch	• Layer 2 switches or a mix of Layer 3 and Layer 2 100/1000BaseT switches with sufficient ports for the controllers and access points • Optical cable (to run from 10GB ports to switch)
Power over Ethernet	Each access point must have access to 802.3af/at-compliant Power over Ethernet (PoE). If this is not provided by the switch, then PoE power injectors can be used between the switch and the access points.
Power	AC power for the switch and the controller.
Null modem cable	DB9 to RJ45 serial console cable
Ethernet cabling	CAT5 Ethernet cable.
Administration console	• Serial terminal running at 115200 baud, 8 bits, no parity, and 1 stop bit (115200 8N1). • After initial configuration, the SSH2 (Secure Shell) protocol or telnet can be used to communicate with the controller.

Element	Requirement
IP settings	IP configuration settings for the blade (static or dynamic IP address and netmask, gateway server)
RADIUS server (optional)	IP address and passphrase for a RADIUS server providing 802.1X security.

Install MC6000 Controller Chassis

Installing an MC6000 chassis is, at minimum, a 2-person task. The base chassis with filler panels weighs approximately 80 pounds, and a fully loaded chassis weighs up to 230 pounds. As such, users should never attempt to install the unit when it contains any blades or power modules pre-installed. At least 2 installers are required to do this task safely.

Perform the procedures in the following sections to install and configure the MC6000 Controller Chassis. The MC6000 Controller Chassis can be set on a flat surface or rack-mounted in a standard 19” telco rack.

Prior to attempting to install the MC6000 chassis itself, be sure to install the required rack-mounted rails in order to properly support the enclosure. The rails are included in the MC6000 packaging and must be assembled separately. Refer to the template provided in the packaging for instructions on properly assembling the rails.

The MC6000 Controller blades and Chassis frame are packaged separately. For the initial installation, use the following procedure:

1. Unpack the shipping containers and verify the following items are included:
   - MC6000 Chassis
   - Two power supply modules
   - Chassis power cord(s)
   - Number of blades that were ordered
   - Software documentation CD
2. Install the MC6000 Chassis in a 19” standard rack (using the provided mounting rails), if desired. The following must be considered when installing the chassis in a rack:
   - Elevated Operating Ambient Temperature—If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra) of 40oC (104oF).

- Reduced Air Flow—Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised. The placeholder blades that come installed with the chassis by default must be left in any unused slots in order to ensure proper airflow.
- Mechanical Loading—Mounting of the equipment in the rack should be such that a hazardous condition is not created due to uneven mechanical loading.
- Circuit Overloading—Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable Earthing—Reliable earthing of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (such as using a power strip and so forth).

3. To install MC6000 Chassis in-rack, move the MC6000 Chassis to the rack or cabinet where it will be installed. Remove any packing materials from the chassis.

Installing an MC6000 chassis is, at minimum, a 2-person task. The base chassis with filler panels weighs approximately 80 pounds, and a fully loaded chassis weighs up to 230 pounds. As such, users should never attempt to install the unit when it contains any blades or power modules pre-installed. At least 2 installers are required to do this task safely.

4. Lift the MC6000 Chassis into position and attach the chassis to the rack rails. Ensure that all mounting screws (both sides) are installed to secure the MC6000 Chassis to the mounting rails.
5. Attach a ground wire to the MC6000 Chassis and to a grounded location.

After the chassis is properly mounted, proceed to the following sections in order to install and configure any blades that have been purchased for it. Note that the chassis should not be plugged in until all blades have been physically installed.

Installing and Configuring MC6000 Blades

Refer to the sections below for instructions on how to install and configure an MC6000 controller blade.

Installing an MC6000 Controller Blade

1. To properly ground yourself, attach a grounding strap to the grounding plug on the front (top left corner) of the MC6000 Chassis.

2. For the slot where the blade will installed, remove the filler panel by pressing the two opposing buttons on the front of the panel. (The buttons must be depressed towards each other.) Pull outwards to slide the panel out. Store the filler panel in a safe place—any chassis slots that are not in use must have a filler panel in place in order to ensure proper airflow.

Electrostatic Discharge—The blades contain ESD-sensitive devices, and can be damaged if not handled in accordance with approved ESD guidelines. Do not remove any blade from its ESD packaging until you are ready to install it in the chassis.

3. The blade has two latches on its face that must be raised in order for it to be locked into the chassis. To raise them, press the sliding top on each latch outward (toward the side of the blade) and then lift the latch away from the blade. Note that there are two small hooks on the end of each latch that fit into a corresponding slot on the blade itself.
4. Carefully align the blade's PCB edges in the bottom and top card guides. Note that the blades can only be installed in one orientation—the "top" of the blade is labeled with a small decal facing upwards. If the blade does not fit properly, verify that you can see the label; if you can't, flip the blade over and try again.
5. Insert the MC6000 blade into the chassis until it makes contact with the backplane connectors. As it seats, the two latches will strike the chassis frame.
6. When the blade has been fully inserted (it should not require a great deal of force to seat it), press the two ejector latches back into place on the front of the blade. The latches hook to the chassis frame itself, so this action will slide and lock it properly into place.
7. Ensure that the two hooks on the latches enter their corresponding slots on the front of the blade. Each hook should click into place when seated.
8. Connect the first optical cable to the primary 10GB port (the top-most port when viewing the blade in the chassis) on the front of the MC6000 blade and to a switch.
9. Configure the Switch settings for connection to MC6000 Blade interfaces running N+1 and/or Dual Ethernet—Redundant mode to the following settings:
    - Spanning Tree link type = Point-to-point
    - MAC aging time for native VLAN of Controller = 10s
    - Forward delay timer for Controller VLAN = 4s
    - Port settings = Portfast
10. Connect the power cords to the power supply modules on back of the chassis and to the wall AC power source. (The MC6000 chassis has two power supplies by default, but can be upgraded to four.) Each power supply has a non-locking 20A 125/230VAC power receptacle with an IEC-320 C19 connector.
11. The unit should power up automatically once the power cords are connected. Ensure that the fans are running, and cool air is flowing through the chassis.
12. Press the power button on the front of the blade.

13. Set up a serial connection from a PC or laptop to the MC6000 Controller blade. For the initial controller configuration, you must connect to the MC6000 Controller blade using the Serial port.
14. On the PC or laptop, set up an ANSI or VT100 compatible terminal session with the following settings:
    - 115200 baud
    - 8 bits
    - no parity
    - 1 stop bit
    - no flow control
15. From the console, initiate the setup command (login and password are both admin), as described in the “Performing an Initial Setup” section of the System Director Getting Started Guide.
16. Perform controller configuration and ESS configuration, as described in the remaining sections of the System Director Getting Started Guide.

Maintaining the MC6000 Chassis

The following tasks may be needed to maintain the MC6000 chassis:

- *“Accessing the Chassis Management Module”* ***on page 69***
- *“Replacing System Modules”* ***on page 73***
- *“Powering Off a Blade”* ***on page 73***
- *“MC6000 Blade Removal”* ***on page 73***
- *“Replacing MC6000 Chassis Power Supplies”* ***on page 74***
- *“LED Status Indicators”* ***on page 76***

Accessing the Chassis Management Module

The Chassis Management Module (CMM) comes pre-installed in the MC6000 chassis. This “command” module communicates with the blade units, the power supplies, and the blade switches. Used in conjunction with the Web Interface management software, the CMM provides administrator control over individual blade units, power supplies, cooling fans and networking switches and monitors onboard temperatures, power status, voltage levels and fan speeds.

The CMM provides a dedicated, local and remote KVM (keyboard/video/mouse) connection over an out of band TCP/IP Ethernet network during any server state (functioning, blue-screen, powered down, BIOS and so on). It also supports Virtual Media (VM) redirection for

CD, floppy and USB mass storage devices and configures such information as the switch IP addresses.

Figure 28: *Chassis Management Module*

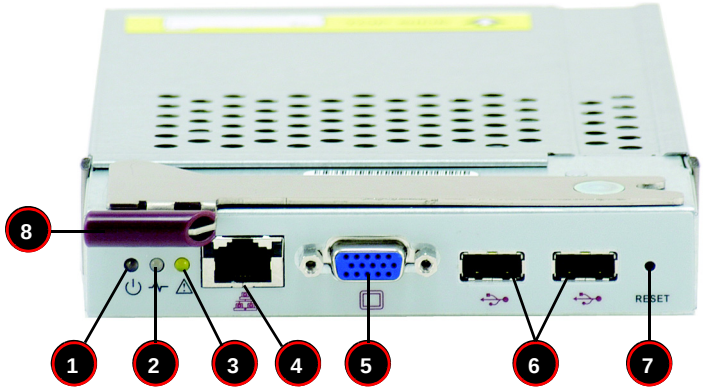


TABLE 9:

Item#	Description
1.	Power LED
2.	Heartbeat LED
3.	Fault LED
4.	Ethernet Port
5.	VGA (Monitor) Port
6.	USB Ports
7.	Reset Button
8.	Module Release Handle

Configuring the CMM

To access/configure the CMM, you first have to configure the IP settings of the CMM depending on you network environment. The below procedure for this configuration just serves as a reference for getting the CMM setup.

Requirements are:

- Computer system running Windows OS with LAN (RJ45) port
- RJ -45 Ethernet cable

The default IP of the CMM is 192.168.100.100. Configure the computer system (connected through Ethernet-LAN to the CMM) to the same address range (for example 192.168.100.101) by following the steps below.

Configuring the CMM in Windows OS:

1. From the computer, go to Start > Control Panel > Network Connections.
2. Right-click on LAN to view properties.
3. Choose “Internet Protocol (TCP/IP)” under the General tab and click on Properties.
4. Manually configure the IP address of the computer system to be in the same address range as the CMM. See the following example:
   - IP address: 192.168.100.101
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.100.1
5. Once the IP address for the computer system is configured, the CMM can be accessed through the web browser by entering the default IP address 192.168.100.100 of the CMM into the browser’s address bar.

Now the module can be configured as desired. This includes changing the CMM’s IP address, subnet mask, and default gateway according to the network environment.

Using the Web-Based Management Utility

The Web-based Management Utility is a web-based interface that consolidates and simplifies system management for the MC6000. The Web-based Management Utility aggregates and displays data from the CMM module. For full documentation of the utility’s interface, refer to the Web-based Management Utility User’s Manual.

The Web-based Management Utility provides the following key management features:

- Enables IT administrators to view in-depth hardware configuration and status information using a single intuitive interface.
- Provides an OS-independent, remote graphical console.
- Allows remote users to map local media (floppy, CD-ROM, removable disks and hard drives) or ISO images on a shared network drive to a blade server.

Supported Browsers

The following browsers have been tested for use with the Web-based Management Utility. It is recommended that you use the most current revision of the browser you choose. The minimum browser revisions supported by the Web-based Management Utility are shown below:

- Internet Explorer 7
- Firefox 2.0.0.7

- Netscape 9.03b

Network Connection/Login

To log into the Web-based Management Utility:

1. Launch a web browser.
2. In the address field of the browser, enter the IP address that you assigned to the Chassis Management Module and press Enter.
3. When the browser makes contact with the Chassis Management Module, enter your username and password, then click Login. The Web-based Management Utility Home Page will then display.

Address Defaults

Table 10 on page 72 shows the default addresses that are initially set for the CMM. Afterwards, you can change these values within the program (see the Web-based Management Utility User's Manual for more details).

TABLE 10: *Address Defaults*

Default	Description
Default IP Address	192.168.100.100
Default Gateway Address	0.0.0.0
Default Subnet Mask	255.255.255.0
Default username	ADMIN
Default password	ADMIN

Resetting the CMM Configuration

The Reset button located on the front of the CMM is used to reset the following software settings to their defaults:

TABLE 11:

Software Setting	Default
User Name and Password	Reset to ADMIN and ADMIN (case sensitive)
IP Address	Reset to 192.168.100.100
Gateway Address	Reset to 0.0.0.0
Subnet Mask	Reset to 255.255.255.0

To reset the CMM to factory defaults, press and hold the Reset button for five seconds.

Replacing System Modules

Use this procedure to install or replace any required modules (such as the CMM or the 10-port 1Gb switch) for the MC6000 chassis. Make sure the cover to the module has been installed before proceeding.

Installing the Module:

1. Remove the dummy cover from the bay you want to place the module in.
2. Place the module's release handle in the open position.
3. Slide the module into the module bay until it stops.
4. Push the release handle to the closed position.
5. After the module has been installed and the handle locked, it will turn on and a POST test will run to verify it is working properly.

Removing the Module:

1. Pull out the release handle to the open position.
2. Pull the module out of the bay.
3. Replace immediately with another module or with a dummy module cover to maintain air-flow integrity.

Powering Off a Blade

Should it become necessary to power off an MC6000 blade, it is recommended you use the CLI command poweroff controller. The command gracefully brings the blade down to a state where power can safely be removed using the power switch.

Failure to use the poweroff command before removing power from the blade can cause flash card corruption and result in the blade becoming non-operational.

MC6000 Blade Removal

To remove an MC6000 blade:

1. Power down the controller using the poweroff controller command (as described in Powering Off a Blade).
2. Wait until the blue LED is fully ON (not blinking); this means that the hot swap sequence is ready for the board removal.
3. Unlock both handle latches by pressing their ends outward (towards the side of the blade) and lifting away from the blade’s face.

4. Use both ejectors to disengage the MC6000 blade from the backplane by pulling it outward.
5. Slide the blade entirely out of the chassis.
6. Replace the blade with the original filler panel by simply sliding it into place and pushing firmly inwards.

Replacing MC6000 Chassis Power Supplies

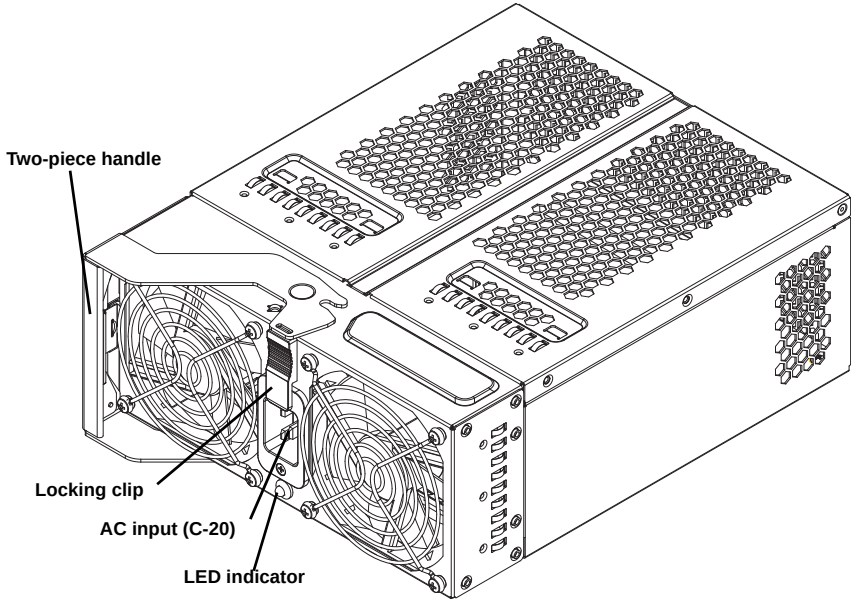
Depending on your configuration, the MC6000 will ship with either two or four power supply modules. By default, it will ship with two; two additional modules can be purchased separately if needed. Follow these instructions for either replacing a faulty power supply or adding a new one to the unit.

When only using two power supplies in your chassis, they should be installed in the bottom two power supply slots in order to optimize airflow. Refer to *Figure 27 on* ***page 64*** for an example of correct installation.

Prior to removing a power supply, ensure that the power cable has been disconnected from the desired module.

For systems using four power supply units simultaneously, the second row of units (on the bottom) will be inserted upside-down when compared to the top row.

Figure 29: *Power Supply Module*



To remove an MC6000 Chassis power supply:

1. Locate the locking clip (indicated in Figure 21) and slide it towards the power connector so that the power supply is no longer locked in place (this mechanism will cause the tab to block the power connector, preventing a module from being removed while still plugged in).
2. Firmly grasp the handle on the power supply and depress the middle portion, disengaging the locking mechanism.
3. Lift the handle outwards (away from the power supply) until the unit starts to slide out from the MC6000.
4. Remove the module completely.

To replace an MC6000 Chassis power supply:

1. Push the replacement power supply into the chassis on the power supply guide rails.
2. Firmly press the power supply handle into the unit until it is flush with the power supply itself. It should lock into place with a light clicking noise.
3. Slide the locking tab into place.

Each power supply unit has two to four rear fans. These fans are not hot-swappable. If one fails, the power supply will continue to operate but you should replace the power supply unit at the earliest opportunity. If two or more fans fail, the power supply unit will shut down and the LED on the back will turn amber.

Power Redundancy

The MC6000 chassis provides space for up to four power supplies. The level of power redundancy this allows varies depending on the number of blades in the unit:

- 0-3 Blades—Two power supplies will provide 1+1 redundancy
- 4-6 Blades—Three power supplies will provide 2+1 redundancy
- 7-10 Blades—Four power supplies will provide 3+1 redundancy

LED Status Indicators

Monitor the status of the blade and the Ethernet connection using the various LED status indicators, located on the front of the blade.

Blade LED Status Indicators

The blade status indicator LEDs are located on the front of the chassis. The description of the LED states are shown in the following tables.

TABLE 12: *MC6000 LED Status Information*

LED	Color	Description
Power	Amber Solid Unlit	Powered on Powered off
Status	Unlit Green	Unimplemented Unimplemented
G1 10G	Unlit Green blinking	No traffic LAN speed 10Gbps
Link/Act	Unlit Green solid Green blinking	Link Down/ No Activity Link Up Rx/Tx Activity

8 Virtual Controller

This guide describes the requirements and installation process for virtual controllers, and includes the following sections:

Virtual Controller Introduction

Virtual controllers are controller images that can be installed on an existing hardware platform provided that the platform implements a supported virtual hosting software solution. The following virtual software platforms are supported:

- VMWare:
  - ESX v4.0 and 4.1
  - ESXi v4.0, 4.1, 5.0, 5.1, 5.5

When a virtual controller is purchased, the controller image can be downloaded from the Customer Support Portal and, once properly installed, can be configured just as a standard physical machine.

Available Virtual Controller Models

The following table lists the controller models available as virtual machines and their corresponding AP/client/throughput maximums.

TABLE 13: *Virtual Controller Options*

Controller Type	Max APs	Max Clients	Max Throughput	Max Throughput (VPN)
MC1500-VE	30	500	800 Mbps	Not supported
MC1550-VE	50	1000	1 Gbps	
MC3200-VE	200	2000	2 Gbps	200 Mbps
MC4200-VE	500	5000	4 Gbps	250 Mbps

Each controller model has specific hardware requirements that must be provided. If these requirements are not met, the installation will fail. See the table below:

TABLE 14: *Virtual Controller Hardware Requirements*

Controller Type	VCPU	Memory	Virtual Ethernet
MC1500-VE	1 core	1GB	2 (active/active), no bonding
MC1550-VE	1 core	2 GB	2 (active/active), no bonding
MC3200-VE	3 cores	2GB	2 (active/active), single bonding
MC4200-VE	4 cores	4GB	4 (active/active), single bonding

Virtual Controller Requirements

The following points are general advisories regarding Virtual Controllers.

- Virtual Controllers essentially act as switches; consequently, their network interfaces **must** be configured for Promiscuous Mode. This will be performed during the controller installation, as detailed in the sections below.
- The number of Virtual Ports configured for the controller will vary depending on the controller's model; be sure to configure the appropriate number of ports for the model being installed. See *Table 14 on page 78* above for details on your controller's required port configuration.
- If you are operating more than one Virtual Controller on a single host machine, ensure that the Virtual Interface for each Virtual Controller is configured in its own port group on the Virtual Switch. This will prevent network loops.
- Virtual Controller Ports must be configured for active-active mode; i.e., active-redundant configuration is not supported.

Performance Recommendations

Virtual NICs (vNIC)

Always use a Gigabit link for the LAN Ports – For optimal performance each vNIC should be connected to a physical interface that is capable of at least 1Gbps.

To get the maximum throughput out of your VE controllers, we don't recommend you share the physical NICs destined for the vNIC interfaces to the controller with any other VM running on the host.

Virtual CPUs (vCPU)

Your VE controller is a network switch that handles every packet on your WLAN network. It is important that the VE Controller receives its recommended share of CPU cycles. To ensure your virtual controller gets its share of CPU cycles, reserve the number of vCPUs recommended for your VE Controller model. Ensure the CPU on the host is server grade

RAM Reservation

Reserve the RAM that is needed by your VE controller model. Provisioning 5% more for the overhead for the VMware overhead makes a significant difference to the performance. For example MC3200-VE model requires 2GB of RAM. Do not over provision your available Physical RAM, the total virtual RAM needed by all running VMs should not exceed the available physical RAM on the system.

Storage

We recommend that you use a disk medium that supports high I/O operations for the datastore VMDK. For example we recommend you use NAS,SAN or dedicated SATA disks. Note, VMware recommends you do not share host physical disks between VMs in order to achieve near-native disk I/O performance. Allocate an unshared disk for the datastore.

Installing a Virtual Controller

Prior to installation, you must have a supported virtual platform already configured and running. Then, simply download the controller image from the Support Portal and copy it to the destination machine. Follow the steps in the section corresponding to your platform below.

VMWare

After downloading the controller image, it must be added to the VMWare management software via the vSphere client. Prior to attempting to configure VMWare to host the controller, it is recommended that you download the virtual controller image (.OVF format) to your local machine. It should be named in the following format:

- meru-[*version*]-[*build*]-[*controller*]V.ovf

In the filename listed above, version will be replaced with the software version number, build with the build number, and controller with the controller model you purchased (e.g., meru-5.2-37-MC4200V.ovf).

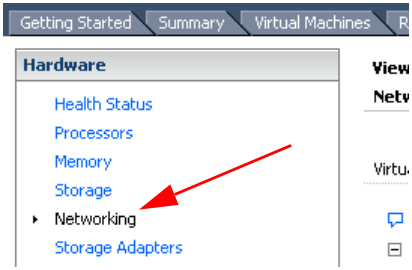
After the download has started, you may proceed to the following steps. The networking components below can be configured during the download, as they are needed for the controller to work properly. The actual installation of the controller is described in *"Creating and Uploading the Controller"* ***on page 82***.

Creating a Virtual Switch

A virtual port group allows configured virtual ports to communicate and be assigned to VLANs. Follow the steps below to configure a group. Note that multiple groups can be created, if desired.

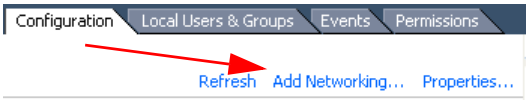
1. From the vSphere Client, select the desired host machine from the left-hand pane and click the **Configuration** tab in the right-hand pane.
2. Click the **Networking** link under the *Hardware* column displayed. This will display a list of all currently configured cards.

Figure 30: *Networking Link*



3. Towards the top-right side of the window, click the **Add Networking…** link to activate the *Add Network Wizard*.

Figure 31: *Add Networking Link*

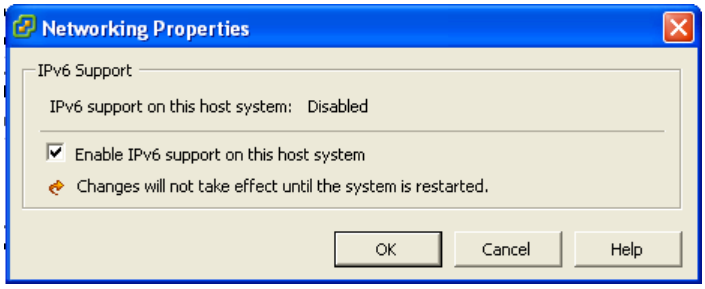


4. Under *Connection Types*, click **Virtual Machine** and click **Next**.
5. Click the **Create a vSphere standard switch** option and click **Next** to proceed to configuring connection settings.
6. Enter a descriptive label for the network in the **Network Label** field.
7. If desired, enable VLAN support on the group by using the **VLAN ID** drop-down to specify **All (4095)**.
8. Click **Next** to view the summary of the configuration changes, then **Finish** to complete the process.

Promiscuous mode is not required to be enabled on the virtual switch; users are advised to configure the switch to Reject Promiscuous Mode requests unless their deployment requires it to be active.

Note that IPv6 support must be enabled on the host machine for virtual controller support. From the networking view, click **Properties** in the top-right of the screen and ensure that the **Enable IPv6 support on this host system** box is checked.

Figure 32: *Networking Properties*



Any changes made to IPv6 support require that the controller be rebooted.

Creating a Port Group

Now that your switch is created, you need to create a port group to control the virtual ports.

1. From the Networking view of the **Configuration** tab, identify the switch you just created from the list displayed and click **Properties…**.
2. From the **Ports** tab, click **Add…**.
3. Select **Virtual Machine** and click **Next**.
4. Enter a name for your port group and specify the VLAN ID to **All**. Click **Next** to continue.
5. Click **Finish** to save the port group.
6. Now that the group has been created, you must enable **Promiscuous Mode** on the group in order for it to operate correctly. Identify the new switch again and click **Properties…**.
7. Select your new port group from the Ports listing and click **Edit**.
8. From the **Security** tab in the resulting window, check the box next to **Promiscuous Mode** and use the drop-down list to specify **Accept**.
9. Click **OK** to save the changes.

Creating and Uploading the Controller

Now that the networking components have been configured and the virtual controller image has been downloaded, you may import the image into the VMWare system and deploy it for use.

1. From the vSphere client interface, select the host machine in the VMWare machine listing on the left of the screen.
2. Click **File>Deploy OVF Template**. The OVF Template wizard starts.
3. In the resulting window, click **Browse…** and navigate to the .ovf file you downloaded in the previous steps.
4. Click **Open** to open the file and **Next** to proceed to the next step in the wizard.
5. The subsequent summary page displays information about the selected .ovf file, including the amount of disk space it will require. Click **Next** to proceed.
6. In the resulting Name and Location screen, you may rename the controller by editing the text in the **Name** field. You may also use the directory tree in the pane below to specify the location you wish to upload the image. Click **Next** when you've made the desired changes.
7. If you have multiple VMware hosts or clusters deployed, select the one you wish to install the controller onto and click **Next**.
8. If desired, select the datastore you wish to use to host the controller image and click **Next**.
9. Use the **Disk Format** window to specify whether your new virtual controller should use thin or thick storage provisioning. Thick provisioning is recommended for virtual controllers.
10. Click **Next** to proceed to the **Network Mapping** window. In the table displayed, click each entry in the **Destination Networks** column and use the resulting drop-down to map each Ethernet port to the virtual switch created in preceding sections. (This step can also be performed later; see *"Configuring Virtual Network Ports"* ***on page 83***).

Note that depending on the virtual controller purchased, you may have either 2 or 4 ports to map:

- MC1500—1-2 ports
- MC1550—1-2 ports
- MC3200—1-2 ports
- MC4200—1-4 ports

11. Click **Next** to proceed and view the summary of the configuration selections made. Click **Finish** to begin deploying the virtual controller.

Configuring Virtual Network Ports

Prior to use, the controller requires that several virtual network ports be created for it to use. The actual number will depend on the controller model purchased:

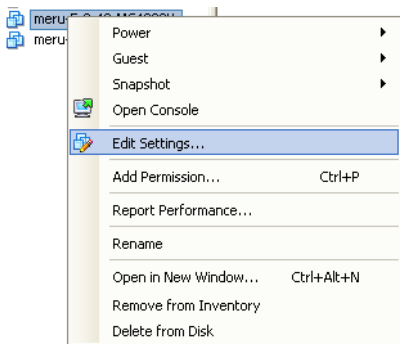
- MC1500—1-2 ports
- MC1550—1-2 ports
- MC3200—1-2 ports
- MC4200—1-4 ports

The steps below will walk you through the process to create a virtual network port. Repeat the steps as many times as needed in until the required number of ports have been configured.

If you already configured the controller's virtual ports in the preceding section, these steps are no longer necessary. Proceed to *"Powering Up the Controller"* ***on page 84***.

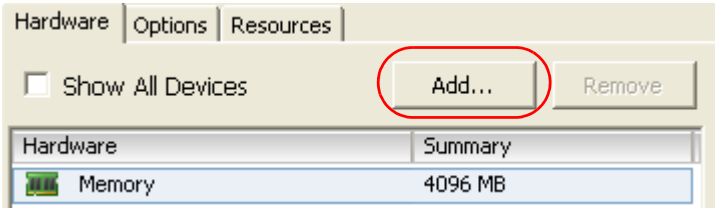
1. From the vSphere Client, right-click the virtual controller to be configured and select **Edit Settings**…. The Virtual Machine Properties window appears.

Figure 33: *Edit VM Settings*



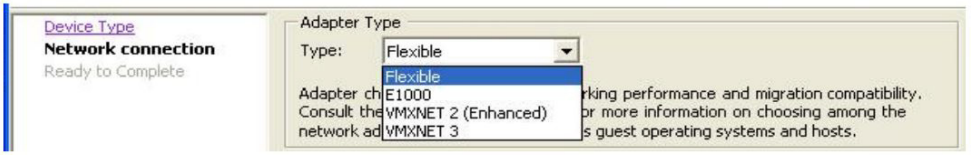
2. Click the **Add…** button to open the Add Hardware window.

Figure 34: *Add Hardware*



3. Click **Ethernet Adapter** in the list of devices available and click **Next**.
4. Use the Adapter Type drop-down list to specify the type of adapter to be used.

Figure 35: *Select Adapter Type*



5. Use the *Network Label* drop-down to select the Virtual Network to which this adapter will be connected.
6. Click **Next** to proceed through the subsequent screens until the final page is reached.
7. Click **Finish** to save the new port.

Powering Up the Controller

Once the controller image has been installed and configured, it is ready to be powered up. From the vSphere Client interface, right-click the controller image in the host listing and select **Power > Power On**. The bootup process can take several minutes; the machine is fully booted when you see a command prompt in the console window.

To access the controller's console, click the Console tab when the controller has been selected. You may initiall login with user name admin, password admin.

At this point, you may open a console session to the controller image and use it to execute the **setup** command to begin configuring the controller. Refer to the instructions provided in the *System Director Getting Started Guide*.

Virtual Controller Licensing

The licensing process differs slightly for virtual controllers in comparison to their physical counterparts. In order to ensure that the license itself remains secure, it is dynamically generated by the Support website based on several server attributes, as listed below:

- Time Zone
- Hostname
- Primary Ethernet IP Address
- Primary Ethernet IP Mask
- Primary Ethernet Gateway Address
- Country Code
- Model Name

Once you have set these options to their desired values, refer to the entitlement certificate provided with your virtual controller software disc and navigate to the Support website supplied. Enter the details listed above into the license generation form in order to create yourlicense. Since the license key is tied to these attributes, they must be fixed prior to requesting a license. If any of these values change, a new license key will need to be generated using the changed value.

Powering Off the Controller

Should it become necessary to power off the controller, use the CLI command **poweroff controller** before using the virtual client software to turn it off. The command gracefully brings the controller down to a state where power can safely be removed using the power switch.

A Cautions and Warnings

The cautions and warnings that appear in this manual are listed below in English, German, French, and Spanish.

Cautions

A Caution calls your attention to a possible hazard that can damage equipment.

"Vorsicht" weist auf die Gefahr einer möglichen Beschädigung des Gerätes in.

Une mise en garde attire votre attention sur un risque possible d'endommagement de l'équipement. Ci-dessous, vous trouverez les mises en garde utilisées dans ce manuel.

Un mensaje de precaución le advierte sobre un posible peligro que pueda dañar el equipo. Las siguientes son precauciones utilizadas en este manual.

	Changes or modifications made to this device that are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. Falls dieses Gerät verändert oder modifiziert wird, ohne die ausdrückliche Genehmigung der für die Einhaltung der Anforderungen verantwortlichen Partei einzuholen, kann dem Benutzer der weitere Betrieb des Gerätes untersagt werden. Les éventuelles modifications apportées à cet équipement sans avoir été expressément approuvées par la partie responsable d'en évaluer la conformité sont susceptibles d'annuler le droit de l'utilisateur à utiliser cet équipement. Si se realizan cambios o modificaciones en este dispositivo sin la autorización expresa de la parte responsable del cumplimiento de las normas, la licencia del usuario para operar este equipo puede quedar anulada.

	Failure to use the poweroff controller command before removing power from the controller can cause Flash card corruption and result in the controller becoming non-operational. Wenn nicht der Befehl poweroff controller vor der Trennung der Stromversorgung vom Controller verwendet wird, kann das eine Korrumpierung der Flash-Karte verursachen, was die Nichtfunktion des Controllers zur Folge haben kann. Il est impératif d'utiliser la commande poweroff controller avant de couper l'alimentation du contrôleur, faute de quoi les données de la carte Flash pourraient être altérées, mettant le contrôleur hors service. Si no se usa el comando poweroff controller antes de desconectar la alimentación del controlador, la tarjeta Flash puede sufrir corrupción y el controlador puede quedar inservible.

	Use only the power cable provided with your Controller. Inspect the power cord and determine if it provides the proper plug and is appropriately certified for use with your electrical system. Discard the cord if it is inappropriate for your country's electrical system and obtain the proper cord from Fortinet, as required by your national electrical codes or ordinances. Es darf nur das Netzkabel, das im Lieferumfang des Controllers enthalten ist, verwendet werden. Inspizieren Sie das Netzkabel und ermitteln Sie, ob es den richtigen Stecker aufweist und zur Verwendung mit Ihrem elektrischen System entsprechend zertifiziert ist. Rangieren Sie das Kabel aus, wenn es nicht für das elektrische System Ihres Landes zugelassen ist, und fordern Sie das richtige Kabel, das den elektrischen Codes oder Vorschriften Ihres Landes entspricht, bei Fortinet an. Utiliser uniquement le cordon d'alimentation électrique fourni avec le contrôleur. Examiner le cordon d'alimentation pour déterminer s'il est doté de la fiche adaptée et s'il est correctement certifié pour une utilisation avec votre système électrique. S'il n'est pas approprié pour le système électrique de votre pays, ne pas utiliser ce cordon et contacter Fortinet pour obtenir le cordon correct , tel qu'il est défini par les réglementations locales. Utilice solamente el cable de alimentación suministrado con su controlador de la serie . Inspeccione el cable de alimentación y determine si tiene el enchufe apropiado y está debidamente homologado para el uso en su sistema eléctrico. Deseche el cable si es inapropiado para el sistema eléctrico de su país y obtenga de Fortinet el cable que cumpla los códigos y ordenanzas eléctricos de su país.

Warnings

A warning calls your attention to a possible hazard that can cause injury or death. The following are the warnings used in this manual.

"Achtung" weist auf eine mögliche Gefährdung hin, die zu Verletzungen oder Tod führen können. Sie finden die folgenden Warnhinweise in diesem Handbuch:

Un avertissement attire votre attention sur un risque possible de blessure ou de décès. Ci-dessous, vous trouverez les avertissements utilisés dans ce manuel.

Una advertencia le llama la atención sobre cualquier posible peligro que pueda ocasionar daños personales o la muerte. A continuación se dan las advertencias utilizadas en este manual.

	ESD protection must be used during hardware installation. Failure to properly use grounding straps when handling the controller could lead to ESD damage. Bei der Hardwareinstallation muss ESD (Electro Static Discharge)-Schutz verwendet werden. Bei nicht ordnungsgemäßer Verwendung von Erdungsbändern bei der Handhabung des Controllers kann ein ESD-Schaden verursacht werden. Durant l'installation du matériel, porter un équipement anti-statique. Toute manipulation du contrôleur sans ruban de mise à la terre est susceptible de l'endommager par électricité statique. Debe usarse protección contra descargas electrostáticas (ESD) durante la instalación del hardware. Si no se utilizan correctamente los correajes de conexión a tierra durante la manipulación del controlador, el operario podría sufrir descargas electrostáticas.

	Any Fast Ethernet (FE) cables installed in air-handling spaces should be suitable under NEC Article 800.50 and marked accordingly for use in plenums and air-handling spaces with regard to smoke propagation, such as CL2-P, CL3-P, MPP (Multi Purpose Plenum), or CMP (Communications Plenum). Alle Fast-Ethernet (FE)-Kabel, die in Lüftungsräumen installiert werden, sollten gemäß NEC Artikel 800.50 geeignet sein und entsprechend zur Verwendung in Hohlräumen (Plenum) und Lüftungsräumen im Hinblick auf Rauchausbreitung gekennzeichnet sein, z.B. CL2-P, CL3-P, MPP (Multi Purpose Plenum) oder CMP (Communications Plenum). Les câbles Fast Ethernet (FE) installés dans un vide d’air doivent correspondre aux critères de l’article 800.50 du code NEC et identifiés en conséquence comme adaptés à une utilisation dans les vides de construction des bâtiments en matière de propagation de la fumée (marquages CL2-P, CL3-P, MPP (Multi Purpose Plenum) ou CMP (Communications Plenum)). Todos los cables Fast Ethernet (FE) instalados en espacios aéreos deben cumplir con el artículo 800.50 del NEC y estar marcados adecuadamente para su uso en espacios aéreos y plenums en lo concerniente a la propagación de humo, tales como CL2-P, CL3-P, MPP (Plenum multifuncional), o CMP (Plenum de comunicaciones).

Inside antennas must be positioned to observe minimum separation of 20 cm. (~ 8 in.) from all users and bystanders. For the protection of personnel working in the vicinity of inside (downlink) antennas, the following guidelines for minimum distances between the human body and the antenna must be observed.

The installation of the indoor antenna must be such that, under normal conditions, all personnel cannot come within 20 cm. (~ 8.0 in.) from any inside antenna. Exceeding this minimum separation will ensure that the employee or bystander does not receive RF-exposure beyond the Maximum Permissible Exposure according to FCC CFR 47, section 1.1310 i.e. limits for General Population/Uncontrolled Exposure.

Innenantennen müssen so positioniert werden, dass ein Mindestabstand von 20 cm (ca. 8 Zoll) zu allen Benutzern und anderen Personen gewahrt wird. Zum Schutz von Personal, das in der Nähe von Innenantennen (Downlink) arbeitet, sind die folgenden Richtlinien für Mindestabstand zwischen dem menschlichen Körper und der Antenne zu beachten.

Die Innenantenne muss so installiert werden, dass sich unter normalen Bedingungen kein Personal bis auf weniger als 20 cm (ca. 8 Zoll) an eine Innenantenne annähern kann. Durch Überschreitung dieses Mindestabstands wird sichergestellt, dass Mitarbeiter oder andere Personen keiner RF-Exposition über die maximal zulässige Exposition (MPE; Maximum Permissible Exposure) gemäß FCC CFR 47, Abschnitt 1.1310 (Grenzwerte für die allgemeine Bevölkerung/unkontrollierte Exposition) ausgesetzt werden.

Les antennes intérieures doivent être positionnées de façon à respecter une distance minimum de 20 cm par rapport aux utilisateurs et aux tiers. Pour la protection du personnel travaillant à proximité des antennes intérieures (liaison descendante), respecter les directives suivantes pour assurer des distances minimales entre les êtres humains et les antennes.

Toute antenne intérieure doit être installée de telle sorte que, dans des conditions normales, le personnel ne puisse s'en approcher à moins de 20 cm. Cette distance minimale est destinée à garantir qu'un employé ou un tiers ne sera pas exposé à un rayonnement radioélectrique supérieur à la valeur maximale autorisée, telle qu'elle est définie dans les limites d'exposition non contrôlées pour la population par la réglementation de la FCC CFR 47, section 1.1310.

Las antenas interiores deben colocarse de manera que se observe una separación mínima de 20 cm. (~ 8 pulg.) respecto a todos los usuarios y circunstantes. Para la protección del personal que trabaje en las inmediaciones de las antenas interiores (receptoras), deben observarse las siguientes directrices relativas a la distancia mínima entre el cuerpo humano y la antena.

La instalación de la antena interior debe efectuarse de tal modo que, en condiciones normales, ningún miembro del personal pueda acercarse a menos de 20 cm. (~ 8,0 pulg.) de cualquier antena interior. El cumplimiento de este mínimo de separación asegura que el empleado o circunstante no recibirá exposición a radiofrecuencia por encima de la Exposición Máxima Permisible conforme a la normativa FCC CFR 47, sección 1.1310, es decir, los límites asignados a la Exposición Incontrolada/Población Civil.

B Safety and Compliance Information

Safety Information

Electrical Cautions

	Use only the power cable provided with your controller. Inspect the power cord and determine if it provides the proper plug and is appropriately certified for use with your electrical system. Discard the cord if it is inappropriate for your country's electrical system and obtain the proper cord from Fortinet, as required by your national electrical codes or ordinances.

Preventing ESD Damage

Electrostatic discharge (ESD) can damage equipment and its electrical circuitry.

	ESD protection must be used during hardware installation. Failure to properly use grounding straps when handling the controller could lead to ESD damage.

Rack-Mount Safety

When installing the controllers into an equipment rack, consider the following to ensure that the controller is operating safely:

- Elevated operating ambient temperature—If you install the controller in a closed or multi-unit rack, the operating ambient temperature of the rack environment might be greater than room ambient temperature. When installing the controller, make sure the environment is compatible with the maximum operating ambient temperature.
- Reduced air flow—Install the controller in a rack so that there is adequate airflow and ventilation for the controller to operate safely.
- Mechanical loading—Make sure the controller is installed so that the mechanical load on the device is evenly distributed.

- Circuit overloading—Consider the connection of the controller to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Consideration should be given to the equipment nameplate ratings.
- Reliable earthing—Maintain reliable earthing of rack-mounted equipment. Pay attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

Compliance Information

All hardware complies with the standards listed in this section.

Electromagnetic Emission

- ICES-003, Electromagnetic Emission
- FCC Part 15 Class A
- EN 55022/CISPR 22 Class A
- VCCI Class A
- EN 61000-3-2, Power Line Harmonics
- EN 61000-3-3, Voltage Fluctuation & Flicker
- EN 61000-6-3, Electromagnetic Compatibility ·

Immunity

- EN 61000-6-1, Electromagnetic Compatibility, Generic Standard
- EN 55024, Immunity Characteristics
- EN 61000-4-2, ESD
- EN 61000-4-3, Radiated, Radio Frequency, Electromagnetic Field
- EN 61000-4-4, Electrical Fast Transient
- EN 61000-4-5, Surge
- EN 61000-4-6, Conducted Disturbances Induced by Radio Frequency Fields
- EN 61000-4-8, Power Frequency Magnetic Field
- EN 61000-4-11, Voltage dips, short interruptions and voltage variations

Safety

- UL 60950-1, first edition

- CSA C22.2 no. 60950-1-03, first edition
- IEC/EN60950-1, first edition

FCC Compliance for Controllers

This equipment has been tested and complies with the requirements for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at his own expense.

Changes or modifications to these products not authorized by Fortinet could void the FCC Certification and negate your authority to operate the product.

Regulatory Information

CISPR 22 CLASS Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take adequate measures.

VCCI

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Japan VCCI

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korea

기 종 별	사 용 자 안 내 문
A급 기기 (업무용 방송통신기기)	이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

MC5000 Compliance Information

All MC5000 hardware complies with the standards listed in this section.

Electromagnetic Emission

- ICES-003, Electromagnetic Emission
- FCC Part 15 Class A
- EN 55022/CISPR 22 Class A
- VCCI Class A
- EN 61000-3-2, Power Line Harmonics
- EN 61000-3-3, Voltage Fluctuation & Flicker
- EN 61000-6-3, Electromagnetic Compatibility

Immunity

- EN 61000-6-1, Electromagnetic Compatibility, Generic Standard
- EN 55024, Immunity Characteristics

- EN 61000-4-2, ESD
- EN 61000-4-3, Radiated, Radio Frequency, Electromagnetic Field
- EN 61000-4-4, Electrical Fast Transient
- EN 61000-4-5, Surge
- EN 61000-4-6, Conducted Disturbances Induced by Radio Frequency Fields
- EN 61000-4-8, Power Frequency Magnetic Field
- EN 61000-4-11, Voltage dips, short interruptions and voltage variations

Safety

- UL 60950-1, first edition
- CSA C22.2 no. 60950-1-03, first edition
- IEC/EN60950-1, first edition

FCC Compliance for Controllers

This equipment has been tested and complies with the requirements for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at his own expense.

Changes or modifications to these products not authorized by Fortinet could void the FCC Certification and negate your authority to operate the product.

CISPR 22 CLASS Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take adequate measures.

Japan VCCI

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

European Union (EU)

This equipment is suitable for connection to an IT system. To ensure safe operation of this equipment, for connection to an IT Power System, provide a protective earth ground connection to the ground stud located at the rear of the unit. Connection to the ground stud is made using a #10 (0.190 in./5mm) ring lug crimped to 12 AWG minimum hook-up wire. Ring lug is secured to stud using the kep nuts.

Controller EIP Tables

Figure 1: *MC3200, MC4200 EIP Table*

有毒有害物质声明 (EIP表)
Hazardous Substance Declaration (EIP table)

Products: MC3200, MC4200, SA2000

部件名称 Item	有毒有害物质或元素的名称及含量 Toxic or Hazardous Substances or Elements					
	铅 Pb	汞 Hg	镉 Cd	六价铬 Cr^{6+}	多溴联苯 PBB	多溴联苯醚 PBDE
印刷电路板组件 Printed Circuit Board Assemblies (PCBA)	X	O	O	O	O	O
配件包 Packing of parts	X	O	O	O	O	O
交换式电源供应器(適配器)/外接式交换式电源供应器(適配器) Power Supply/Adapter	X	O	O	O	O	O

O: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006 标准规定的限量要求以下。

O: Indicates all homogeneous materials hazardous substances content are below the SJ/T 11363-2006 MCV limit.

X: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006 标准规定的限量要求。

X: Indicates that the hazardous substance content contained in any one of the homogeneous materials of the part exceeded the MCV limits specified in the Standard SJ/T 11363-2006.

Figure 2: *MC1550 EIP Table*

有毒有害物质声明 (EIP表)

Hazardous Substance Declaration (EIP table)

Products: MC1550, SA250

部件名称 Item	有毒有害物质或元素的名称及含量 Toxic or Hazardous Substances or Elements					
	铅 Pb	汞 Hg	镉 Cd	六价铬 Cr^{6+}	多溴联苯 PBB	多溴联苯醚 PBDE
机构材料–机箱/面板 Mech. Parts - Chassis / panel	O	O	O	O	X	X
机构材料–铁件/螺丝及其他 Mech. Parts - Metal bracket / Screws etc.	O	O	O	O	X	X
机构材料–散热片 Mech. Parts – Heatsink	O	O	O	O	X	X
机板 PCBA board	O	O	O	O	O	O
电池 Battery	O	O	O	O	O	O
线材 Cable	O	O	O	O	O	O
硬盘 HDD	O	O	O	O	O	O
驱动光盘 Driver CD	O	O	O	O	O	O
纸箱 Carton	O	O	O	O	O	O
缓冲包材/塑料袋 EPE / bag	O	O	O	O	O	O
电源供应器 Power Adapter	O	O	O	O	O	O

O: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006 标准规定的限量要求以下。

O: Indicates all homogeneous materials hazardous substances content are below the SJ/T 11363-2006 MCV limit.

X: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006 标准规定的限量要求。

X :Indicates that the hazardous substance content contained in any one of the homogeneous materials of the part exceeded the MCV limits specified in the Standard SJ/T 11363-2006.